

SPHEREON 4300

McDATA®
Sphereon™ 4300 Fabric Switch
Installation and Service Manual

P/N 620-000171-010
REV A

Simplifying Storage Network Management

Record of Revisions and Updates

Revision	Date	Description
620-000171-000	8/2003	General availability (GA) release of the manual.
620-000171-010	12/2003	Revision of the manual to describe Release 6.1 of the Enterprise Operating System.
620-000171-020	1/2005	Revision of the manual to describe Release EOS 7.0.

Copyright © 2003-2005 McDATA Corporation. All rights reserved.

Printed January 2005

Third Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without prior written consent of McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer applications, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer applications described in this document. McDATA Corporation retains all rights, title, and interest in the computer applications.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer applications described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

Preface	xiii
----------------------	------

Chapter 1 General Information

Switch Description.....	1-1
Field-Replaceable Units	1-3
Power Supply	1-4
Controls, Connectors, and Indicators	1-5
IML/Reset Button.....	1-5
Ethernet LAN Connector.....	1-6
Power and System Error LEDs	1-6
Port Status LEDs	1-6
Maintenance Port.....	1-6
Switch Specifications	1-7
Maintenance Approach.....	1-8
Switch Management.....	1-9
Error-Detection, Reporting, and Serviceability Features	1-10
Software Diagnostic Features.....	1-11
SANpilot Interface	1-11
SNMP Trap Message Support	1-13
Tools and Test Equipment.....	1-13
Tools Supplied with the Switch	1-14
Tools Supplied by Service Personnel	1-15

Chapter 2 Installation Tasks

Factory Defaults	2-1
Installation Options	2-2
Summary of Installation Tasks.....	2-2
Task 1: Verify Installation Requirements	2-3

Task 2: Unpack, Inspect, and Install the Switch	2-3
Unpack and Inspect the Switch	2-4
Desktop Installation	2-4
Rack-Mount Installation	2-5
Task 3: Configure the Switch at the SANpilot Interface.....	2-6
Configure Switch Ports	2-8
Configure BB Credit	2-10
Configure Switch Identification	2-11
Configure Date and Time	2-13
Configure Operating Parameters	2-14
Configure Fabric Parameters	2-16
Configure Network Information	2-19
Configure SNMP	2-21
Enable or Disable the CLI and SSH	2-23
Enable or Disable OSMS and Host Control	2-24
Change User Password.....	2-25
Configure Port Binding	2-26
Configure Switch Binding.....	2-27
Configuring the Switch Binding Membership List	2-31
Configure Fabric Binding	2-32
Enable or Disable Enterprise Fabric Mode	2-34
Configure OpenTrunking	2-35
Install PFE Keys (Optional).....	2-38
Task 4: Configure Switch Network Information (Optional)....	2-39
Task 5: Cable Fibre Channel Ports	2-45
Task 6: Configure Zoning (Optional).....	2-46
Configure Zones	2-46
Configure Zone Sets	2-49
Task 7: Connect Switch to a Fabric Element (Optional)	2-51
Task 8: Register with the McDATA File Center	2-52

Chapter 3 **Diagnostics**

Maintenance Analysis Procedures	3-1
Factory Defaults.....	3-1
Quick Start	3-2
MAP 0000: Start MAP	3-6
MAP 0100: Power Distribution Analysis	3-18
MAP 0200: POST Failure Analysis	3-21
MAP 0300: Loss of Web Browser PC Communication	3-23
MAP 0400: FRU Failure Analysis	3-30
MAP 0500: Port Failure and Link Incident Analysis	3-35
MAP 0600: Fabric, ISL, and Segmented Port Problem	

Determination	3-54
---------------------	------

Chapter 4 **Repair Information**

Procedural Notes	4-2
Obtain Log Information	4-2
Event Log	4-3
Open Trunking Re-Route Log	4-4
Link Incident Log	4-5
Viewing the Security Log	4-6
Viewing the Audit Log	4-7
Viewing the Fabric Log	4-8
Viewing the Embedded Port Frame Log	4-9
Viewing All Logs	4-10
Obtain Port Diagnostic Information	4-11
Port LEDs	4-11
SANpilot Interface	4-13
Perform Port Diagnostic Loopback Tests	4-19
Internal Loopback Test	4-19
External Loopback Test	4-21
Collect Maintenance Data	4-22
Set the Switch Online or Offline	4-25
Set Online State	4-25
Set Offline State	4-26
Block or Unblock a Port	4-26
Block a Port	4-26
Unblock a Port	4-28
Clean Fiber-Optic Components	4-28
Power-On Procedure	4-29
Power-Off Procedure	4-30
IML or Reset the Switch	4-30
Switch IML	4-31
Switch Reset	4-31
Manage Firmware Versions	4-32
Determine Switch Firmware Version	4-32
Add a Firmware Version to the Browser PC Hard Drive ..	4-33
Download a Firmware Version to the Switch	4-38
Reset Configuration Data	4-40

Chapter 5 **FRU Removal and Replacement**

Procedural Notes	5-1
RRP 1: SFP Optical Transceiver	5-2

Chapter 6 Illustrated Parts Breakdown

Front-Accessible FRUs6-2

Miscellaneous Parts6-3

Power Cords and Receptacles.....6-4

Appendix A Event Code Tables

System Events (000 through 199)A-2

Fan Events (300 through 399)A-20

CTP Card Events (400 through 499)A-23

Port Events (500 through 599)A-29

Thermal Sensor Events (800 through 899)A-37

Index..... 1

Figures

1-1	Sphereon 4300 Switch	1-2
1-2	Sphereon 4300 Switch (Front View)	1-3
1-3	Sphereon 4300 Switch (Rear View)	1-3
1-4	View Panel (SANpilot Interface)	1-12
1-5	Loopback Plug	1-14
1-6	Fiber-Optic Protective Plug	1-14
1-7	Null Modem Cable	1-15
2-1	AC Power Connection	2-5
2-2	Enter Network Password Dialog Box	2-7
2-3	View Panel (Switch Page)	2-8
2-4	Configure Panel (Ports Page)	2-9
2-5	Configure BB Credits	2-11
2-6	Configure Panel (Switch Page with Identification Tab)	2-12
2-7	Configure Panel (Switch Page with Date/Time Tab)	2-13
2-8	Configure Panel (Switch Page with Parameters Tab)	2-14
2-9	Configure Panel (Switch Page with Fabric Parameters Tab)	2-17
2-10	Configure Panel (Switch Page with Network Tab)	2-19
2-11	Network Information Message Box	2-20
2-12	Configure Panel (Management Page with SNMP Tab)	2-22
2-13	Configure Panel (Management Page with CLI Tab)	2-24
2-14	Configure Panel (Management Page with OSMS Tab)	2-25
2-15	Configure Panel (Security Page with User Rights Tab)	2-26
2-16	Configure Panel (Security Page with Port Binding Tab)	2-27
2-17	Configure Panel (Security Page with Switch Binding Tab)	2-30
2-18	Configure Panel (Security Page with Fabric Binding Tab)	2-33
2-19	Configure Panel (Security Page with EFM Tab)	2-35
2-20	Configure Panel (Performance Page with OpenTrunking Tab)	2-36
2-21	Operations Panel (Feature Installation Tab)	2-38
2-22	Connection Description Dialog Box	2-41
2-23	Connect To Dialog Box	2-42

2-24	COMn Properties Dialog Box	2-42
2-25	Sphereon 4300 - HyperTerminal Window	2-43
2-26	HyperTerminal Dialog Box (1)	2-44
2-27	HyperTerminal Dialog Box (2)	2-45
2-28	Configure Panel (Zoning Page with Zones Tab)	2-47
2-29	Configure Panel (Zoning Page with Modify Zone Tab)	2-48
2-30	Configure Panel (Zoning Page with Zone Set Tab)	2-50
2-31	McDATA File Center Home Page	2-52
2-32	McDATA File Center (New User Registration Page)	2-54
3-1	Username and Password Required Dialog Box	3-7
3-2	View Panel (SANpilot Interface)	3-8
3-3	View Panel (Port Properties Tab)	3-10
3-4	View Panel (FRU Properties Tab)	3-12
3-5	Monitor Panel (Logs Page)	3-13
3-6	Event Log	3-14
3-7	Connection Description Dialog Box	3-26
3-8	Connect To Dialog Box	3-27
3-9	COMn Properties Dialog Box	3-28
3-10	Sphereon 4300 - HyperTerminal Dialog Box	3-29
3-11	HyperTerminal Dialog Box	3-29
3-12	HyperTerminal Dialog Box	3-30
3-13	Link Incident Log	3-42
4-1	Monitor Panel (Logs Page)	4-3
4-2	Event Log	4-3
4-3	Open Trunking Re-Route Log	4-4
4-4	Link Incident Log	4-5
4-5	Security Log	4-6
4-6	Viewing the Audit Log	4-7
4-7	Viewing the Fabric Log	4-8
4-8	Viewing the Frame Log	4-9
4-9	Setting Embedded Port Frame Filtering	4-10
4-10	All Logs View	4-11
4-11	Monitor Panel (Port List Page)	4-14
4-12	Monitor Panel (Port Stats Page)	4-15
4-13	View Panel (Port Properties Page)	4-18
4-14	Operations Panel (Port Page with Diagnostics Tab)	4-20
4-15	Operations Panel (Maintenance Page with System Files Tab)	4-23
4-16	Save As Dialog Box	4-24
4-17	Download Complete Dialog Box	4-24
4-18	Operations Panel (Switch Page with Online State Tab)	4-26
4-19	Configure Panel (Ports Page)	4-27
4-20	Clean Fiber-Optic Components	4-28
4-21	View Panel (Unit Properties Page)	4-32

4-22	McDATA File Center Home Page	4-33
4-23	McDATA File Center (Login Page)	4-34
4-24	McDATA File Center (Find Documents Page)	4-34
4-25	McDATA File Center (Documents Match Page)	4-35
4-26	McDATA File Center (Current Request Page)	4-35
4-27	McDATA File Center (Request History Page)	4-36
4-28	File Download Dialog Box	4-36
4-29	Save As Dialog Box	4-37
4-30	Download Complete Dialog Box	4-37
4-31	Operations Panel (Maintenance Page with Firmware Upgrade Tab) .	4-38
4-32	Browser-Specific Message Box	4-39
4-33	Firmware Received Message Box	4-39
4-34	Firmware Upgrade Complete Message Box	4-40
4-35	Operations Panel (Switch Page with Reset Config Tab)	4-41
4-36	Browser-Specific Message Box	4-42
5-1	SFP Optical Transceiver Removal and Replacement	5-3
6-1	Front-Accessible FRUs	6-2
6-2	Miscellaneous Parts	6-3
6-3	Power Cords and Receptacles	6-4

2-1	Factory-Set Defaults (Sphereon 4300 Switch)	2-1
2-2	Installation Task Summary	2-2
3-1	Factory-Set Defaults	3-2
3-2	MAP Summary	3-2
3-3	Event Codes versus Maintenance Action	3-3
3-4	MAP 200 Event Codes	3-22
3-5	MAP 200 Byte 0 FRU Codes	3-22
3-6	MAP 400 Event Codes	3-31
3-7	MAP 500 Event Codes	3-35
3-8	Port Operational States and Actions	3-38
3-9	Invalid Attachment Reasons and Actions	3-45
3-10	MAP 600 Event Codes	3-55
3-11	Port Segmentation Reasons and Actions	3-56
3-12	Byte 4 Segmentation Reasons and Actions	3-59
3-13	Bytes 8 through 11 Failure Reasons and Actions	3-66
4-1	Port Operational States	4-12
6-1	Front-Accessible FRU Parts List	6-2
6-2	Miscellaneous Parts List	6-3
6-3	Power Cord and Receptacle List	6-5

This publication is part of a documentation suite that supports the McDATA® Sphereon 4300 Fabric Switch.

Who Should Use this Manual



Use this publication if you are a trained installation and service representative experienced with the switch, storage area network (SAN) technology, and Fibre Channel technology.

The Sphereon 4300 Fabric Switch contains no customer-serviceable parts that require internal access to the product during normal operation or prescribed maintenance conditions. In addition, refer to this manual for instructions prior to performing any maintenance action.

Organization of this Manual

This publication includes six chapters and four appendices organized as follows:

Chapter 1, *General Information* - This chapter describes the switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications. The chapter also describes the maintenance approach, switch management through the SANpilot interface, error detection and reporting features, serviceability features, software diagnostic features, and tools and test equipment.

Chapter 2, *Installation Tasks* - This chapter describes tasks to install, configure, and verify operation of the switch.

Chapter 3, *Diagnostics* - This chapter describes maintenance analysis procedures (MAPs) to fault isolate a switch problem to an individual FRU.

Chapter 4, *Repair Information* - This chapter describes supplementary diagnostic and repair procedures for a failed switch. The chapter includes procedures to display and use log information, perform port diagnostics, manage configuration data, collect maintenance data, power-on, power-off, and reset the switch, set the switch online or offline, block ports, manage switch firmware, and clean fiber optics.

Chapter 5, *FRU Removal and Replacement* - This chapter describes procedures to remove and replace switch FRUs.

Chapter 6, *Illustrated Parts Breakdown* - This chapter illustrates, describes, and shows the location of switch FRUs. In addition, switch FRUs are cross-referenced to corresponding part numbers.

Appendix A, *Event Code Tables* - This appendix provides an explanation of event codes that appear at the SANpilot interface. The event severity and a recommended course of action in response to each event are also provided.

An ***Index*** is also provided.

Related Publications

Other publications that provide additional information about the switch include:

- *McDATA Products in a SAN Environment - Planning Manual* (626-000124).
- *McDATA SANpilot User Manual* (620-000160).
- *McDATA SNMP Support Manual* (620-000131).
- *McDATA E/OS Command Line Interface User Manual* (620-000134).
- *McDATA Sphereon 4300 and 4500 Switch Rack-Mount Kit Installation Instructions* (958-000316).
- *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100).

Ordering Printed Manuals

To order a paper copy of this manual, submit a purchase order as described in *Ordering McDATA Documentation Instructions*, which is found on McDATA's web site, **<http://www.mcdata.com>**. To obtain documentation CD-ROMs, contact your sales representative.

Where to Get Help

For technical support, contact the McDATA Solution Center. The center provides a single point of contact for assistance, and is staffed 24 hours a day, seven days a week, including holidays. Contact the center at the phone number, fax number, or e-mail address listed

below. Please have the product serial number (printed on the service label attached to the switch) available.

Phone: (800) 752-4572 or (720) 566-3910

Fax: (720) 566-3851

E-mail: support@mcddata.com

Forwarding Publication Comments

We welcome comments about this publication. Please send comments to the McDATA Solution Center by telephone, fax, or e-mail. The numbers and e-mail address are listed above. Please identify the manual, page numbers, and details.

Trademarks

The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation or SANavigator, Inc. in the United States or other countries or both:

Registered Trademarks

McDATA®

Fabricenter®

OPENready®

SANavigator®

Trademarks

Sphereon™

Networking the world's
business data™

OPENconnectors™

SANpilot™

SANtegrity™

EON™

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States or other countries or both.

Laser Compliance Statement



Laser transceivers for the switch are tested and certified in the United States to conform to Title 21 of the Code of Federal Regulations (CFR), Subchapter J, Parts 1040.10 and 1040.11 for Class 1 laser products. Elsewhere, the transceivers are tested and certified to be compliant with International Electrotechnical Commission IEC825-1 and European Norm EN60825-1 and EN60825-2 regulations for Class 1 laser products. Class 1 laser products are not considered hazardous. The transceivers are designed such that there is never human access to laser radiation above a Class 1 level during normal operation or prescribed maintenance conditions.

Federal Communications Commission (FCC) Statement

The switch generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with instructions provided, may cause interference to radio communications. The product was tested and found to comply with the limits for Class A computing devices pursuant to Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a commercial environment. Operation of the product in a residential area is likely to cause interference in which case the user, at his or her own expense, will take whatever measures are required to correct the interference. Any modifications or changes made to the product without explicit approval from McDATA, by means of a written endorsement or through published literature, will invalidate the service contract and void the warranty agreement with McDATA.

Chinese National Standards Mark

The Chinese National Standards (CNS) mark illustrated below indicates switch compliance with Taiwanese Bureau of Standards, Metrology, and Inspection (BSMI) regulatory requirements.

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

European Union Conformity Declarations for Information Technology Equipment

The switch meets the following regulatory requirements as set forth by European Norms (ENs) and relevant International Electrotechnical Commission (IEC) standards for commercial and light industrial information technology equipment (ITE).

- **EN55022: 1998; EN55024: 1997, +A1: 1998:** ITE-generic radio frequency interference (RFI) emission standard for domestic, commercial, and light industrial environments.
- **EN60950:** ITE-generic electrical and fire safety standard for domestic, commercial, and light industrial environments.

European Union Directives

The European Union (EU) Council has implemented a series of directives that define product safety standards for all EU member countries. The following directives apply to the switch:

- The product conforms with all protection requirements of EU directive 89/336/EEC (EMC Directive) in accordance with the laws of the member countries relating to electromagnetic compatibility (EMC), emissions, and immunity.
- The product conforms with all protection requirements of EU directive 73/23/EEC (Low Voltage Directive) in accordance with the laws of the member countries relating to electrical safety.
- The product conforms with all protection requirements of EU directive 93/68/EEC (Machinery Directive) in accordance with the laws of the member countries relating to safe electrical and mechanical operation of the equipment.

McDATA does not accept responsibility for any failure to satisfy the protection requirements of any of these directives resulting from a non-recommended or non-authorized modification to a switch.

Danger and Attention Statements

The following **DANGER** statement appears in this publication and describes safety practices that must be observed while installing or servicing the switch. A **DANGER** statement provides essential information or instructions for which disregard or noncompliance may result in death or severe personal injury. The **DANGER** statement appears in English, followed by translations to:

- Chinese (simplified - People's Republic of China).
- Chinese (traditional - Taiwan).
- French (European).
- German.

- Hebrew.
- Italian.
- Portuguese.
- Spanish (European).
- Spanish (Latin American).



DANGER

Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.



危險

使用所提供的电源线。确保使用正确型号的设备电源插座，提供必需的电压并且正确接地。



危險

使用隨附的電源線，確定使用正確類型的設備電源插座，提供必需的電壓，並且正確接地。



DANGER

Utiliser les câbles d'alimentation fournis. S'assurer que la prise de courant du local est du type correct, délivre la tension requise et est correctement raccordée à la terre.



GEFAHR

Die mitgelieferten Netzkabel verwenden. Sicherstellen, dass die verwendete Netzsteckdose dem vorgeschriebenen Typ entspricht, die erforderliche Spannung liefert und einwandfrei geerdet ist.

סכנה



השתמש בכבלי החשמל הנלווים. וודא כי כלי הקיבול לחשמל של המתקן הוא מהסוג הנכון, מספק את המתח הדרוש, ומוארק כהלכה.



PERICOLO

Usare il cavo di alimentazione in dotazione. Assicurarsi che la presa di corrente a disposizione sia del tipo corretto, eroghi la tensione richiesta e sia dotata di messa a terra idonea.



PERIGO

Use os cordões elétricos fornecidos. Certifique-se de que o tipo de receptor de energia da facilidade é apropriado, fornece a voltagem necessária, e está corretamente aterrado.



PELIGRO

Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea el tipo correcto, suministre el voltaje necesario, y que esté apropiadamente puesto a tierra.



PELIGRO

Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea del tipo correcto, suministre el voltaje necesario, y que esté apropiadamente conectado a tierra.

The following **ATTENTION** statements appear in this publication and describe practices that must be observed while installing or servicing the switch. An **ATTENTION** statement provides essential information or instructions for which disregard or noncompliance may result in equipment damage or loss of data.

ATTENTION ! Prior to servicing a product, determine the Ethernet LAN configuration. Installation of products on a public customer intranet can complicate problem determination and fault isolation.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

General Precautions

When installing or servicing the product, follow these practices:

- Always use correct tools.
- Always use correct replacement parts.
- Keep all paperwork up to date, complete, and accurate.

ESD Precautions

All electrostatic discharge (ESD) sensitive components and FRUs in the product are enclosed and shielded. ESD procedures are not required when working with the product.

The McDATA® Sphereon™ 4300 Fabric Switch provides up to 12 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric devices or arbitrated loop devices. This function allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment.

This chapter describes the switch and switch management through the SANpilot™ interface. The chapter specifically describes:

- The switch, including field-replaceable units (FRUs), controls, connectors, and indicators, and switch specifications.
- Maintenance approach.
- Switch management through the SANpilot interface.
- Error detection, reporting, and serviceability features.
- Software diagnostic features.
- Tools and test equipment.

Switch Description

The Sphereon 4300 Switch provides Fibre Channel device connectivity through 12 ports that operate at either 1.0625 or 2.125 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for up to 12 switched fabric devices.
- Fabric loop ports (FL_Ports) to provide arbitrated loop connectivity and fabric attachment for FC-AL devices. Each FL_Port can theoretically support the connection of 126 FC-AL devices.
- Expansion ports (E_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches. E_Port connectivity is not standard, and must be configured through an optional product feature enablement (PFE) key.

The switch can be installed on a table or desk top, mounted in a McDATA FC-512 Fabriccenter[®] equipment cabinet, or mounted in any standard 19-inch equipment rack. [Figure 1-1](#) illustrates the switch.

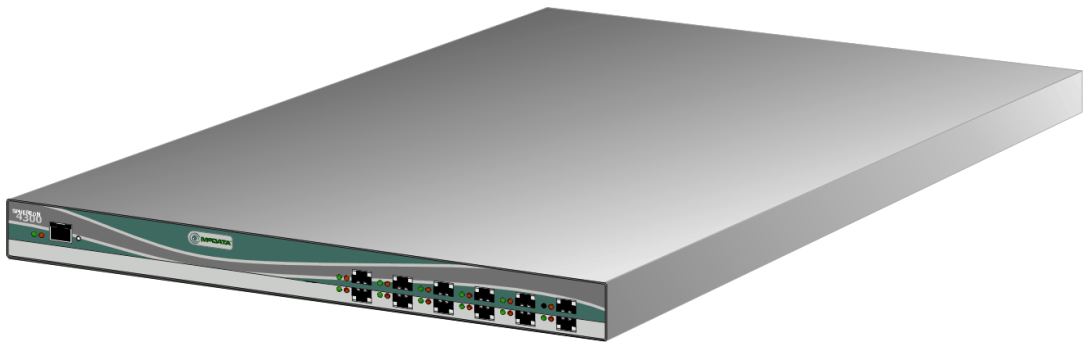


Figure 1-1 Sphereon 4300 Switch

Administrators or operators with a browser-capable PC and an Internet connection monitor and manage the switch through the SANpilot interface. The SANpilot interface manages only a single switch, and provides a graphical user interface (GUI) that supports product configuration, statistics monitoring, and basic operation. The SANpilot interface is opened from a standard web browser running Netscape Navigator[®] 4.6 or higher or Microsoft[®] Internet Explorer 4.0 or higher. At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password.

Field-Replaceable Units

The switch provides a modular design that enables quick removal and replacement of small form factor pluggable (SFP) optical transceivers. [Figure 1-2](#) illustrates the front of the switch. SFP optical transceivers are the only FRUs. The figure also shows front-panel controls, connectors, and indicators.

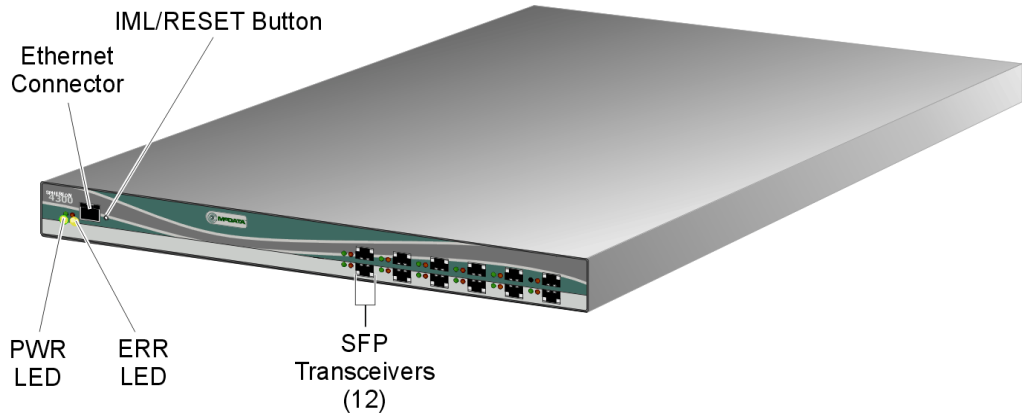


Figure 1-2 Sphereon 4300 Switch (Front View)

[Figure 1-3](#) illustrates the rear of the switch. The figure shows the power connector and maintenance port.

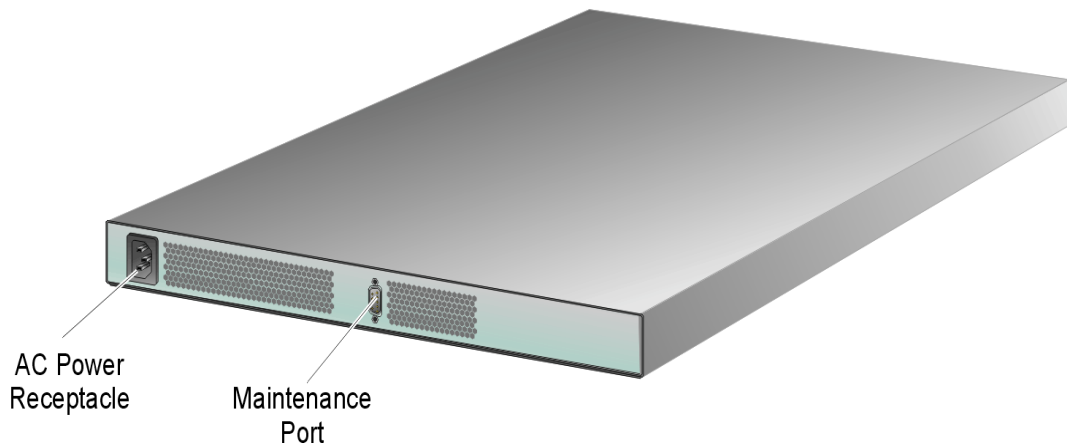


Figure 1-3 Sphereon 4300 Switch (Rear View)

SFP Transceiver

Singlemode or multimode fiber-optic cables attach to switch ports through SFP transceivers. The fiber-optic transceivers provide duplex LC[®] connectors, and can be detached from switch ports (through a 10-pin interface) for easy replacement. The following fiber-optic transceiver types are available:

- **Shortwave laser (1.0625 Gbps)** - Shortwave laser transceivers provide connections for transferring 1.0625 Gbps data over short distances as follows:
 - Up to 500 meters through 50-micron multimode fiber.
 - Up to 300 meters through 62.5-micron multimode fiber.
- **Shortwave laser (2.125 Gbps)** - Shortwave laser transceivers provide connections for transferring 2.125 Gbps data over short distances as follows:
 - Up to 300 meters through 50-micron multimode fiber.
 - Up to 150 meters through 62.5-micron multimode fiber.
- **Longwave laser (1.0625 Gbps)** - Longwave laser transceivers provide connections for transferring 1.0625 Gbps data up to 10 kilometers through 9-micron singlemode fiber.
- **Longwave laser (2.125 Gbps)** - Longwave laser transceivers provide connections for transferring 2.125 Gbps data up to 10 kilometers through 9-micron singlemode fiber.
- **Extended longwave laser (2.125 Gbps)** - Two types of extended longwave laser transceivers provide connections for transferring 2.125 Gbps data up to 20 kilometers or 35 kilometers through 9-micron singlemode fiber.

Power Supply

The switch contains one power supply with two internal cooling fans. The assembly is not a FRU. The power supply steps down and rectifies facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the control processor (CTP) card. The power supply also provides input filtering, overvoltage protection, and overcurrent protection, and is input rated at 100 to 240 volts alternating current (VAC).

Three cooling fans (two integrated in the power supply) provide cooling for the power supply and CTP card, as well as redundancy for continued operation if a single fan fails.

Controls, Connectors, and Indicators

Controls, connectors, and indicators for the switch include the:

- Combined initial machine load and reset (**IML/RESET**) button.
- Ethernet LAN connector.
- Green power (**PWR**) and amber system error (**ERR**) light-emitting diodes (LEDs).
- Green, blue, and amber status LEDs associated with Fibre Channel ports.
- RS-232 maintenance port.

IML/Reset Button

When the **IML/RESET** button ([Figure 1-2](#) on page 1-3) is pressed, held for three seconds, and released, the switch performs an IML that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic.

When the **IML/RESET** button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the **ERR** LED blinks at twice the unit beaoning rate. A reset is disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the SANpilot interface connection to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

A reset should only be performed if a CTP card failure is indicated. As a precaution, the **IML/RESET** button is flush mounted to protect against inadvertent activation.

Ethernet LAN Connector

The front panel provides a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector (Figure 1-2 on page 1-3) that attaches to an Ethernet LAN to provide communication with a PC accessing the SANpilot interface or a simple network management protocol (SNMP) management workstation. The connector provides two green LEDs. The left LED illuminates to indicate LAN operation at 10 Mbps, while the right LED illuminates to indicate LAN operation at 100 Mbps.

Power and System Error LEDs

The **PWR** LED (Figure 1-2 on page 1-3) illuminates when the switch is connected to facility AC power and is operational (the switch does not have a power switch). If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The **ERR** LED (Figure 1-2 on page 1-3) illuminates when the switch detects an event requiring immediate operator attention, such as a FRU failure or link incident. The LED remains illuminated as long as an event is active. The LED extinguishes when *Clear System Error Light* is selected from the SANpilot interface.

The LED blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing. The LED also blinks (at twice the beaconing rate) when the **IML/RESET** button is pressed and held for more than three seconds.

Port Status LEDs

Amber and green/blue LEDs to the left of each port (Figure 1-2 on page 1-3) illuminate, extinguish, or blink to indicate port status and port speed. The amber LED illuminates if the port fails. The green/blue LED illuminates green to indicate 1.0625 Gbps port operation. The green/blue LED illuminates blue to indicate 2.125 Gbps port operation.

Maintenance Port

The rear panel provides a 9-pin DSUB maintenance port (Figure 1-3 on page 1-3) that provides a connection for a local terminal or dial-in connection for a remote terminal. Although the port is typically used by authorized maintenance personnel, operations personnel can use the port to configure switch network addresses.

Switch Specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances for the Sphereon 4300 Switch.

Physical Characteristics

Dimensions:

Height: 4.1 centimeters (1.6 inches) or 1 rack unit

Width: 43.7 centimeters (17.2 inches)

Depth: 47.3 centimeters (18.6 inches)

Weight: 6.8 kilograms (15 pounds)

Power requirements:

Input voltage: 100 to 240 VAC

Input frequency: 47 to 63 Hz

Plan for single phase or phase-to-phase connections and 5-ampere dedicated service

Heat dissipation:

37 watts (127 BTUs/hr)

Cooling airflow clearances (switch chassis):

Right and left side: 1.3 centimeters (0.5 inches)

Front and rear: 7.6 centimeters (3.0 inches)

Top and bottom: No clearance required

Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical noise:

64 dB "A" scale

Inclination:

10⁰ maximum

Storage and Shipping Environment

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

Shipping temperature:

-40⁰ F to 140⁰ F (-40⁰ C to 60⁰ C)

Storage temperature:

34⁰ F to 140⁰ F (1⁰ C to 60⁰ C)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

84⁰ F (29⁰ C)

Altitude:

40,000 feet (12,192 meters)

Operating Environment**Temperature:**

40⁰ F to 104⁰ F (4⁰ C to 40⁰ C)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

81⁰ F (27⁰ C)

Altitude:

10,000 feet (3,048 meters)

Maintenance Approach

Whenever possible, the switch maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications. Switch fault isolation begins when one or more of the following occur:

- System event information displays at the SANpilot interface.
- LEDs on the switch front panel or adjacent to Fibre Channel ports illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.

System events can be related to a:

- Switch failure (hardware or software).
- Ethernet LAN communication failure between the switch and a PC accessing the SANpilot interface.
- Link failure between a port and attached device.
- ISL failure or segmentation of an E_Port.

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information is provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system event information, isolate a switch failure, repair the switch, and verify switch operation. The fault isolation process normally begins with *MAP 0000: Start MAP* on page 3-6.

Ensure the correct switch is selected for service by enabling unit beaconing at the failed switch. The amber system error (**ERR**) LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Switch Management

The switch is managed and controlled through a customer-supplied PC platform with an Internet connection to the SANpilot interface on the switch. Using this graphical user interface (GUI), operators can quickly view switch status. The interface also allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. FRU status and system alert information are highly visible.

With switch firmware Version 4.0 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the switch through the SANpilot interface. The application provides a GUI that supports switch configuration, operation, performance monitoring, maintenance and diagnostic functions.

The SANpilot interface is opened from a standard web browser running Netscape Navigator® Version 4.6 (or higher) or Microsoft Internet Explorer Version 4.0 (or higher). At the browser, enter the IP address of the switch as the Internet uniform resource locator (URL).

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on the switch and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- FRUs (SFP transceivers) that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of tools or equipment.
- System alerts and logs that display switch and Fibre Channel link status at the SANpilot interface.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.

- Data collection through the SANpilot interface to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.

- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- SNMP management using the Fibre Channel Fabric Element MIB (Version 1.1), Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the SANpilot interface to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.

Software Diagnostic Features

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- SFP transceivers provide on-board diagnostic and monitoring circuits that continuously report status to the SANpilot interface. The interface provides system alerts and logs that display failure and diagnostic information.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.

SANpilot Interface

The SANpilot interface provides a GUI accessed through the Internet (locally or remotely) to manage, monitor, and isolate problems for the Sphereon 4300 Switch. When the interface opens, the default display is the *View* panel ([Figure 1-4](#) on page 1-12).

Task selection tabs appear at the top of the panel, a graphical representation of the switch hardware (front only) appears at the right side of the panel, and menu selections (*View*, *Configure*, *Monitor*, *Operations*, and *Help*) appear at the left side of the panel.

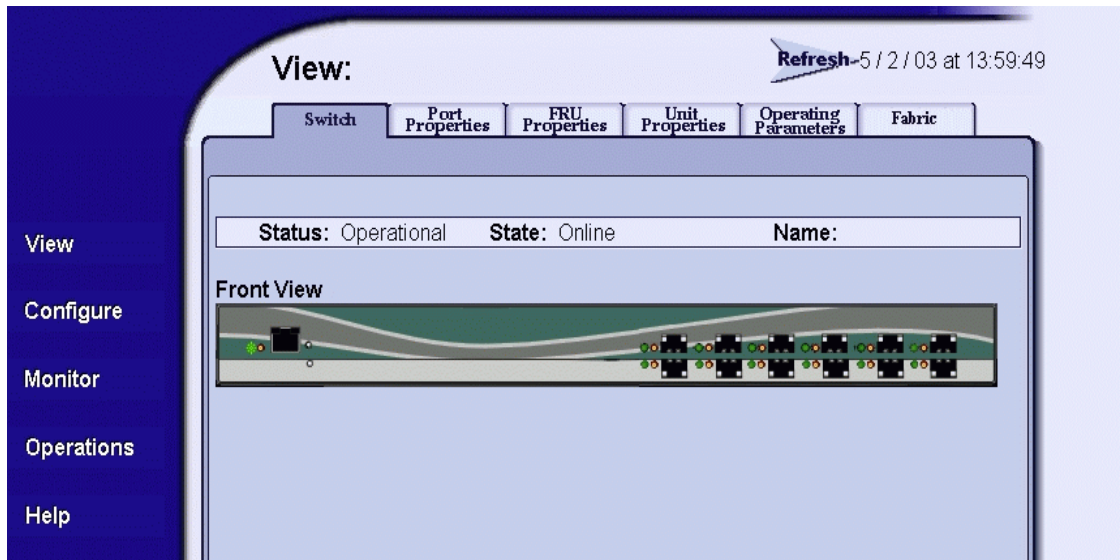


Figure 1-4 View Panel (SANpilot Interface)

The task selection tabs allow personnel to perform switch-specific tasks, and are a function of the menu selected as follows:

- **View** - At the *View* panel, the *Switch* (default), *Port Properties*, *FRU Properties*, *Unit Properties*, *Operating Parameters*, and *Fabric* task selection tabs appear.
- **Configure** - At the *Configure* panel, the *Ports* (default), *Switch*, *Management*, *Zoning*, *Security*, and *Performance* task selection tabs appear.
- **Monitor** - At the *Monitor* panel, the *Port List* (default), *Port Stats*, *Log*, and *Node List* task selection tabs appear.
- **Operations** - At the *Operations* panel, the *Switch* (default), *Port*, *Maintenance*, and *Feature Installation* task selection tabs appear.
- **Help** - The *Help* selection opens online user documentation that supports the SANpilot interface.

SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate switch operational state changes or failure conditions can be customer-configured to be transmitted to up to 12 management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each switch. If installed on a customer intranet, the workstations communicate with switches through the browser-capable PC.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC 1157), and a custom, switch-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customer personnel only, the messages may be provided to service personnel as initial notification of a switch problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart** - reports that the SNMP agent is reinitializing due to a switch reset.
- **warmStart** - reports that the SNMP agent is reinitializing due to a switch reset or initial program load (IPL).
- **authorizationFailure** - reports attempted access by an unauthorized SNMP manager. This trap is configurable and is disabled by default.

Switch-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the SANpilot interface, users at SNMP management workstations can modify MIB variables. For additional information, refer to the *McDATA OPENconnectors SNMP Support Manual* (620-000131).

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch. These tools are supplied with the switch or must be supplied by service personnel.

Tools Supplied with the Switch

The following tools are supplied with the switch. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Loopback plug** - An SFP multimode (shortwave laser) or singlemode (longwave laser) loopback plug (Figure 1-5) is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed.

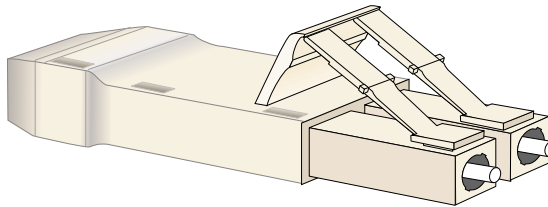


Figure 1-5 Loopback Plug

- **Fiber-optic protective plug** - For safety and port transceiver protection, fiber-optic protective plugs (Figure 1-6) must be inserted in all switch ports without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports.

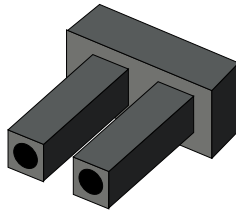


Figure 1-6 Fiber-Optic Protective Plug

- **Null modem cable** - An asynchronous RS-232 null modem cable (Figure 1-7 on page 1-15) is required to configure switch network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors.

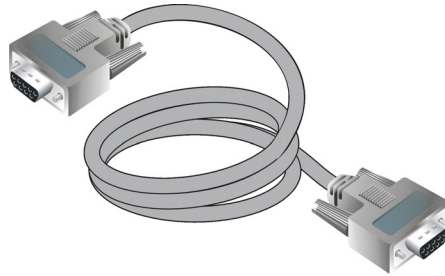


Figure 1-7 Null Modem Cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation or maintenance actions. Use of the tools may be required to perform one or more test, service, or verification tasks.

- **Scissors or pocket knife** - A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking replacement FRUs.
- **Cross-tip (#2 Phillips) screwdriver** - The screwdriver is required to rack-mount the switch or tighten various chassis or cabinet components.
- **T10 Torx® tool** - The tool is required to rack-mount the switch or tighten various chassis or cabinet components.
- **Maintenance terminal (desktop or notebook PC)** - The PC is required to configure switch network addresses and acquire event log information through the maintenance port. The PC must have:
 - The Microsoft Windows 98, Windows 2000, Windows XP, or Millennium Edition operating system installed.
 - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit** - The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

This chapter describes tasks to install, configure, and verify operation of the Sphereon 4300 Switch and SANpilot interface. The switch can be installed on a table top, mounted in a McDATA FC-512 Fabriccenter equipment cabinet, or mounted in any standard 19-inch equipment rack.

Factory Defaults

[Table 2-1](#) lists factory-set defaults for the Sphereon 4300 Switch.

Table 2-1 Factory-Set Defaults (Sphereon 4300 Switch)

Item	Default
SANpilot interface user name (case sensitive)	Administrator
SANpilot interface password (case sensitive)	password
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Installation Options

The switch is installed in one of three configurations. The options are:

- **Table or desktop** - One or more switches are delivered and installed at the customer facility on a table or desktop. Ethernet cabling, distance, and local area network (LAN) addressing issues must be considered.
- **Fabriccenter equipment cabinet** - One or more switches are delivered (cabled and installed) in a McDATA equipment cabinet. Ethernet cabling, distance, and LAN addressing issues must only be considered if multiple cabinets are daisy-chained.
- **Customer-supplied equipment rack** - One or more switches are delivered to the customer facility for installation in a customer-supplied equipment rack. Rack mount flanges and hardware are provided in the shipping containers. Ethernet cabling, distance, and LAN addressing issues must be considered.

Summary of Installation Tasks

[Table 2-2](#) summarizes installation tasks for the switch. The table describes each task, states if the task is required or optional, and lists the page reference.

Table 2-2 **Installation Task Summary**

Task Number and Description	Required or Optional	Page
<i>Task 1: Verify Installation Requirements.</i>	Required.	2-3
<i>Task 2: Unpack, Inspect, and Install the Switch.</i>	Required.	2-3
<i>Task 3: Configure the Switch at the SANpilot Interface.</i>	Required.	2-6
<i>Task 4: Configure Switch Network Information (Optional).</i>	Optional - configure if connecting multiple switches to a public LAN.	2-39
<i>Task 5: Cable Fibre Channel Ports.</i>	Required.	2-45
<i>Task 6: Configure Zoning (Optional).</i>	Optional - perform this task to configure zoning.	2-46
<i>Task 7: Connect Switch to a Fabric Element (Optional).</i>	Optional - perform this task to connect the switch to a Fibre channel fabric.	2-51
<i>Task 8: Register with the McDATA File Center.</i>	Required.	2-52

Task 1: Verify Installation Requirements

Verify the following requirements are met prior to switch and SANpilot interface installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to *McDATA Products in a SAN Environment - Planning Manual* (626-000124) for information.
- Storage area network (SAN), director, fabric switch, and Fibre Channel arbitrated loop (FC-AL) device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *McDATA Products in a SAN Environment - Planning Manual* (626-000124) for information.
- A browser-capable PC and Internet connectivity is available to support switch management through the SANpilot interface.
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables are delivered and available. Ensure the cables are the correct length with the required connectors.
- A customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a corporate or dedicated LAN.

Task 2: Unpack, Inspect, and Install the Switch

The following paragraphs provide instructions to unpack and inspect one or more Sphereon 4300 Switches, and install the switches in a desktop or rack-mount configuration.

If the switch is delivered as part of an FC-512 Fabriccenter equipment cabinet, refer to the *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100) for instructions. Go to [Task 3: Configure the Switch at the SANpilot Interface](#) on page 2-6.

Unpack and Inspect the Switch

Unpack and inspect the switch(es) as follows:

1. Inspect shipping container(s) for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack shipping container(s) and inspect each item for damage. Ensure the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, contact the McDATA solution center as follows:

Phone: (800) 752-4572 or (720) 566-3910

Fax: (720) 566-3851

E-mail: support@mcddata.com

Desktop Installation

To install the switch on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of the switch. Ensure the pads are aligned with the scribed circles at each corner.
2. Position the switch on a table or desktop as directed by the customer. Ensure:
 - A grounded AC electrical outlet is available.
 - Adequate ventilation is present, and areas with excessive heat, dust, or moisture are avoided.
 - All planning considerations are met. Refer to *McDATA Products in a SAN Environment - Planning Manual* (626-000124) for information.
3. Verify all small form factor pluggable (SFP) optical transceivers are installed as ordered.
4. Connect the AC power cord to the receptacle at the rear of the chassis as shown in [Figure 2-1](#) on page 2-5.
5. Connect the AC power cord to a facility power source that provides single-phase, 100 to 240 volt alternating current (VAC) current.

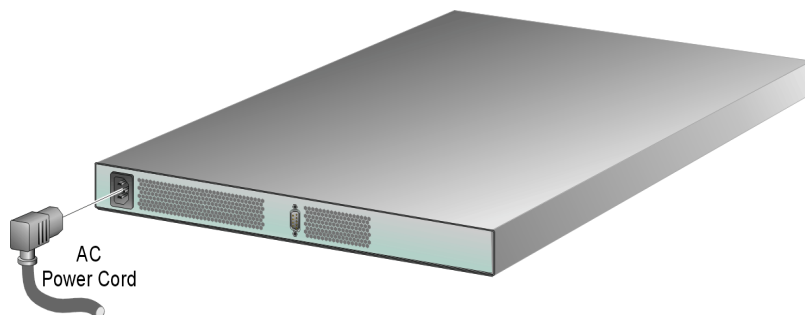


Figure 2-1 AC Power Connection

6. When the power cord is connected, the switch powers on and performs power-on self-tests (POSTs). During POSTs:
 - a. The green power (**PWR**) LED on the front panel illuminates.
 - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
 - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - d. The green/blue and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
7. After successful POST completion, the green power (**PWR**) LED remains illuminated and all other front panel LEDs extinguish.
8. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
9. Go to [Task 3: Configure the Switch at the SANpilot Interface](#) on page 2-6.

Rack-Mount Installation

Perform the following steps to install and configure the switch in a Fabriccenter equipment cabinet or a customer-supplied equipment rack. An optional rack-mount kit, T10 Torx tool, and #2 Phillips screwdriver are required.

1. Locate the rack-mount position as directed by the customer. The switch is 1.75 inches, or 1U high.
2. Verify all SFP optical transceivers are installed as ordered.

3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.
4. Using a T10 Torx tool and #2 Phillips screwdriver, install the switch in the equipment cabinet. Refer to the *Sphereon 4300 Switch Rack-Mount Kit Installation Instructions* (958-000316) for guidance.
5. Connect the AC power cord to the receptacle at the rear of the chassis as shown in [Figure 2-1](#) on page 2-5.
6. Connect the AC power cord to a facility power source that provide single-phase, 100 to 240 VAC current.
7. When the power cord is connected, the switch powers on and performs POSTs. During POSTs:
 - a. The green power (**PWR**) LED on the front panel illuminates.
 - b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
 - c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - d. The green/blue and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
8. After successful POST completion, the green power (**PWR**) LED remains illuminated and all other front panel LEDs extinguish.
9. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
10. Go to [Task 3: Configure the Switch at the SANpilot Interface](#) below.

Task 3: Configure the Switch at the SANpilot Interface

To configure the Sphereon 4300 Switch from the SANpilot interface, selectively perform the following configuration tasks according to the customer's installation requirements:

- Configure switch ports.
- Configure the switch identification, date and time, operating parameters, fabric parameters, and network addresses.
- Configure SNMP trap message recipients, enable the command line interface (CLI), and configure the open systems management server (OSMS) feature.

- Configure administrator and operator passwords.
- Install switch product feature enablement (PFE) keys.

Perform procedures under this task to configure the switch from the SANpilot interface. A PC platform with Internet access and standard web browser running Netscape Navigator 4.6 or higher or Microsoft Internet Explorer 4.0 or higher is required.

1. Connect the switch to the Internet or Ethernet LAN segment as follows:
 - a. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labelled **10/100**) on the left front of the switch chassis.
 - b. Connect the remaining end of the Ethernet cable to an Internet port or Internet-connected LAN segment as directed by the customer's network administrator.
2. Open the SANpilot interface as follows:
 - a. Ensure the browser-capable PC and the Ethernet LAN segment (with the Sphereon 4300 Switch attached) are connected through the Internet. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
 - b. At the browser, enter the Internet Protocol (IP) address of the switch as the Internet uniform resource locator (URL). Use the default IP address of **10.1.1.10**. The *Enter Network Password* dialog box displays (Figure 2-2).



Figure 2-2 Enter Network Password Dialog Box

- c. Type the default user name and password.

NOTE: The default SANpilot interface user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- d. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed (Figure 2-3).

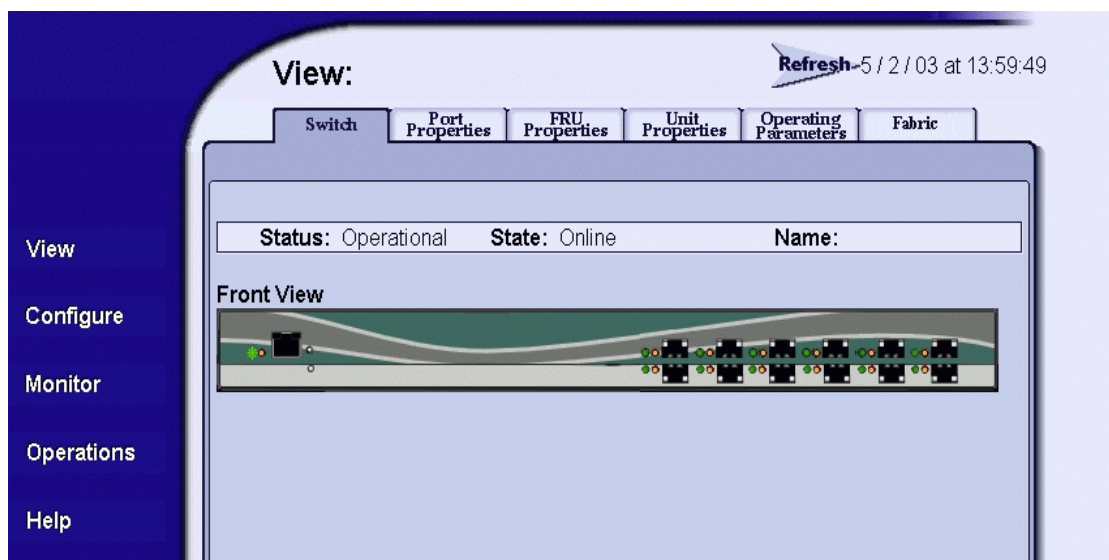


Figure 2-3 View Panel (Switch Page)

Configure Switch Ports

Perform procedures in this section to configure names and operating characteristics for Fibre Channel ports. To configure one or more switch ports:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed with *Basic Info* selected. (Figure 2-4 on page 2-9).

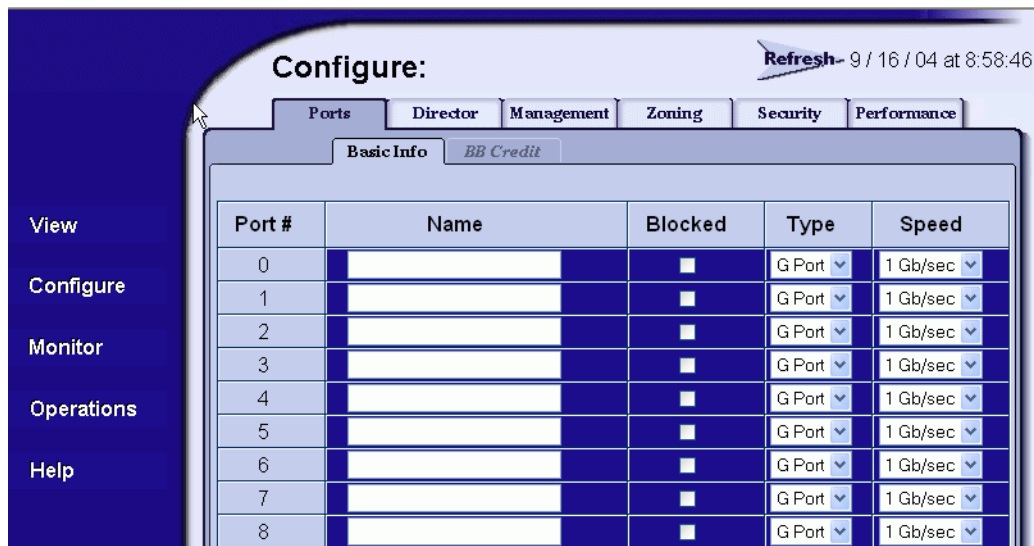


Figure 2-4 Configure Panel (Ports Page)

- a. For each port to be configured, type a port name of 24 alphanumeric characters or less in the associated *Name* field. The port name should characterize the device to which the port is attached.
- b. Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).
- c. Click the check box in the *FAN* column to enable or disable the fabric address notification (FAN) feature (default is enabled). A check mark in the box indicates FAN is enabled. When the feature is enabled, the port transmits FAN frames after loop initialization to verify that FC-AL devices are still logged in. It is recommended this option be enabled for ports configured for loop operation.

- d. Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
 - Fabric port (**F_Port**).
 - Expansion port (**E_Port**). This selection is available only if enabled through an optional PFE key.
 - Generic port (**G_Port**). A generic port setting allows F_Port and E_Port behavior only. This selection is available only if enabled through an optional PFE key.
 - Generic mixed port (**GX_Port**). A generic mixed port setting allows F_Port, fabric loop port (FL_Port), and E_Port behavior. This selection is available only if enabled through an optional PFE key.
 - Fabric mixed port (**FX_Port**). A fabric mixed port setting allows F_Port and FL_Port behavior only.
- e. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are:
 - Auto-negotiate between 1.0625 and 2.125 gigabit per second (Gbps) operation (**Negotiate**). This is the default selection.
 - 1.0625 Gbps operation (**1 Gb/sec**).
 - 2.125 Gbps operation (**2 Gb/sec**).
2. Click *Activate* to save and activate the changes. The message **Your changes to the port configuration have been successfully activated** appears.

Configure BB Credit

Perform this procedure to configure the BB Credit allocation for all ports on the product. For each type of port, there is a maximum and minimum BB Credit limit which is displayed as a range. To configure the BB Credit allocation, the port must be set to offline. The simplest way to set the port to offline is to block the port. As you enter the BB Credit value, the value will be validated and an error message will be displayed for each port if applicable. The BB Credit configuration will not be activated if there are any outstanding errors.

To configure BB credits:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 2-4). Select the *BB Credits* tab is selected. Use the vertical scroll bar to display additional port information rows.
2. It is recommended you select the Default values. If not, you can enter values in the RX BB Credit field.
3. Select Activate to save the changes.
4. Place the port back online.

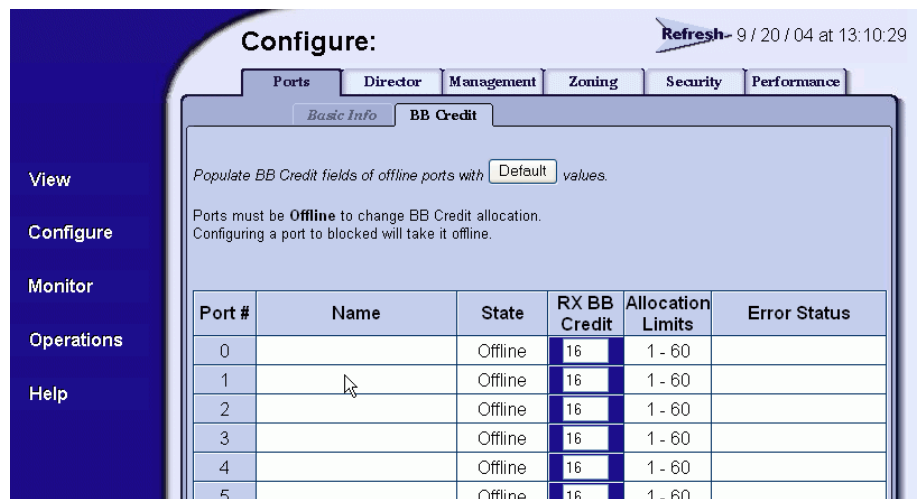


Figure 2-5 Configure BB Credits

Configure Switch Identification

Perform this procedure to configure the switch name, description, location, and contact person. The *Name*, *Location*, and *Contact* variables configured here correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed switches. To configure the switch identification:

1. At the *Configure* panel, click the *Switch* tab. The *Switch* page displays with the *Identification* tab selected (Figure 2-6 on page 2-12).

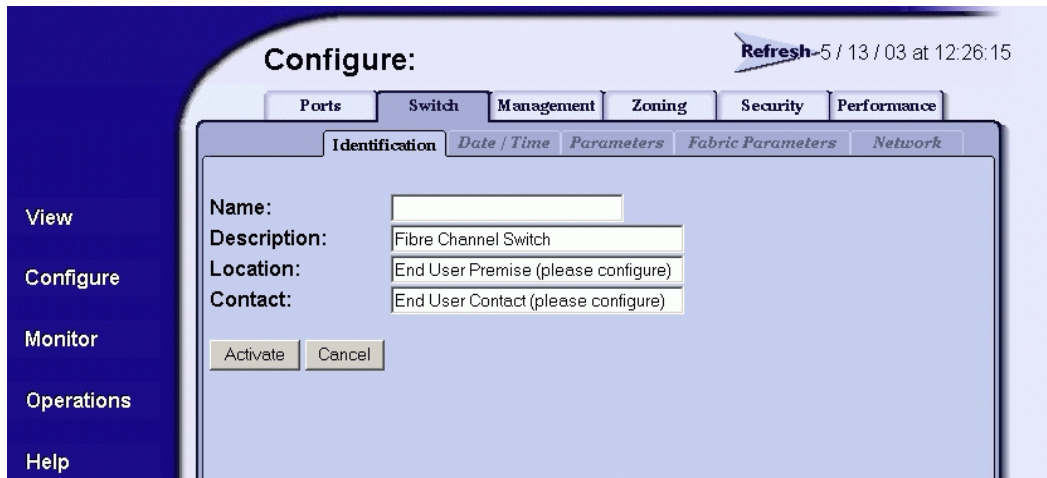


Figure 2-6 Configure Panel (Switch Page with Identification Tab)

- a. Type a switch name of 24 alphanumeric characters or less in the *Name* field. Each switch should be configured with a unique name.

If the switch is installed on a public LAN, the name should reflect the switch's Ethernet network domain name system (DNS) host name. For example, if the DNS host name is **sphereon4300.mcdata.com**, the name entered in this dialog box should be **sphereon4300**.
 - b. Type a switch description of 255 alphanumeric characters or less in the *Description* field.
 - c. Type the switch's physical location (255 alphanumeric characters or less) in the *Location* field.
 - d. Type the name of a contact person (255 alphanumeric characters or less) in the *Contact* field.
2. Click *Activate* to save and activate the changes. The message **Your changes to the identification configuration have been successfully activated** appears.

Configure Date and Time

Perform this procedure to configure the effective date and time for the switch. To set the date and time:

1. At the *Configure* panel, click the *Date/Time* tab. The *Switch* page displays with the *Date/Time* tab selected (Figure 2-7).

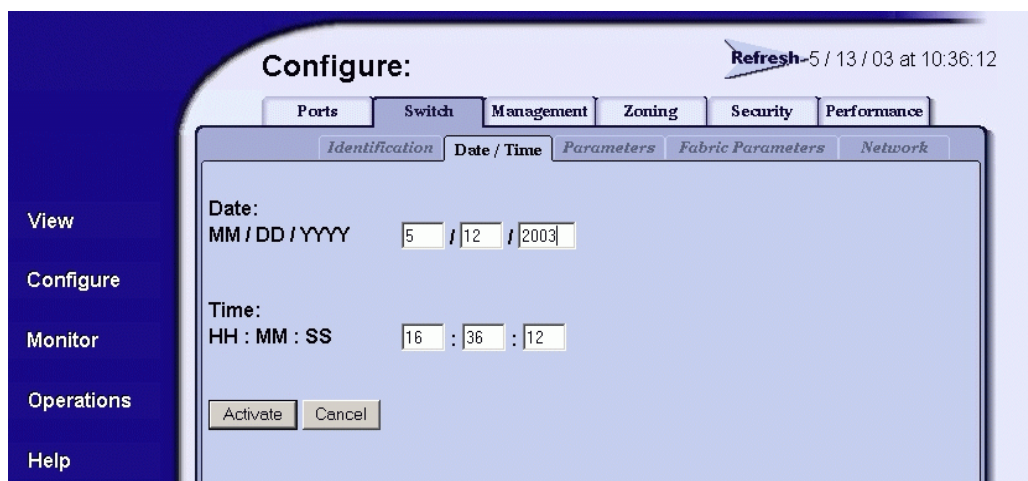


Figure 2-7 Configure Panel (Switch Page with Date/Time Tab)

- a. Click the *Date* fields that require change, and type numbers in the following ranges:
 - Month (MM): 1 through 12.
 - Day (DD): 1 through 31.
 - Year (YYYY): greater than 1980.
 - b. Click the *Time* fields that require change, and type numbers in the following ranges:
 - Hour (HH): 0 through 23.
 - Minute (MM): 0 through 59.
 - Second (SS): 0 through 59.
2. Click *Activate* to save and activate the changes. The message **Your changes to the date/time configuration have been successfully activated** appears.

Configure Operating Parameters

Perform this procedure to configure the switch's preferred domain ID, insistent domain ID, rerouting delay, and domain registered state change notifications (RSCNs). The switch must be set offline to configure the preferred domain ID. To configure parameters:

1. Set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Switch* tab, then click the *Parameters* tab. The *Switch* page displays with the *Parameters* tab selected (Figure 2-8).

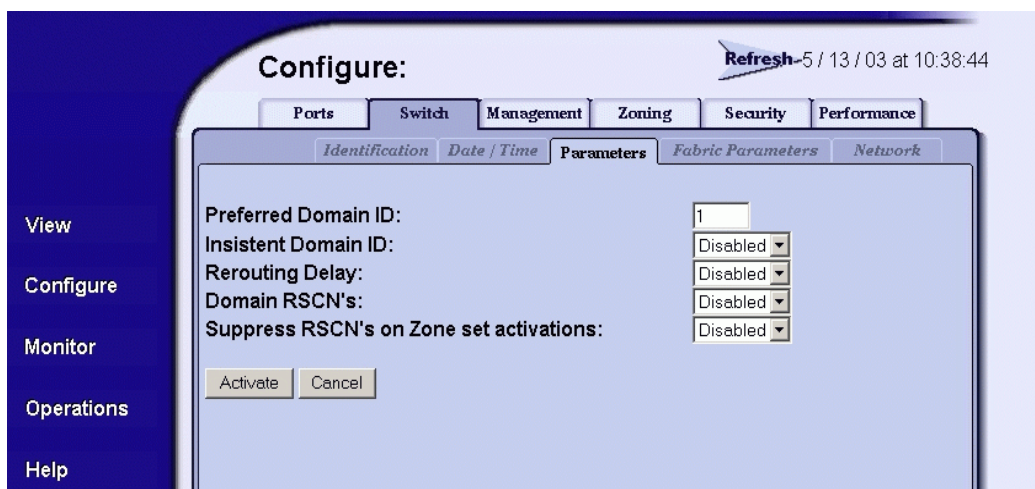


Figure 2-8 Configure Panel (Switch Page with Parameters Tab)

- a. At the *Preferred Domain ID* field, type a value between 1 through 31. The domain ID uniquely identifies each switch in a fabric.

NOTE: If the switch is attached to a fabric element, the switch and element must have unique domain IDs. If the values are not unique, the E_Port connection to the element segments and the switch cannot communicate with the fabric.

- b. At the *Insistent Domain ID* field, select *Enabled* or *Disabled*. When this parameter is enabled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Insistent Domain ID must be enabled.

- c. At the *Rerouting Delay* field, select *Enabled* or *Disabled*. When this parameter is enabled, traffic is delayed through the fabric by the specified error detect time out value (E_D_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Rerouting Delay must be enabled.

- d. At the *Domain RSCNs* field, select *Enabled* or *Disabled*. When this parameter is enabled, attached devices can register to receive notification when another attached device changes state.

NOTE: If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Domain RSCN must be enabled.

4. Click *Activate* to save and activate the changes. The message **Your changes to the operating parameters configuration have been successfully activated** appears.
5. If fabric parameters require configuration, go to [Configure Fabric Parameters](#) below. If the configuration is complete, set the switch online as follows:

- a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
- b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value (R_A_TOV), E_D_TOV, switch priority, and interop mode. The switch must be set offline. To configure parameters:

1. If required, set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Switch* tab, then click the *Fabric Parameters* tab. The *Switch* page displays with the *Fabric Parameters* tab selected (Figure 2-9).

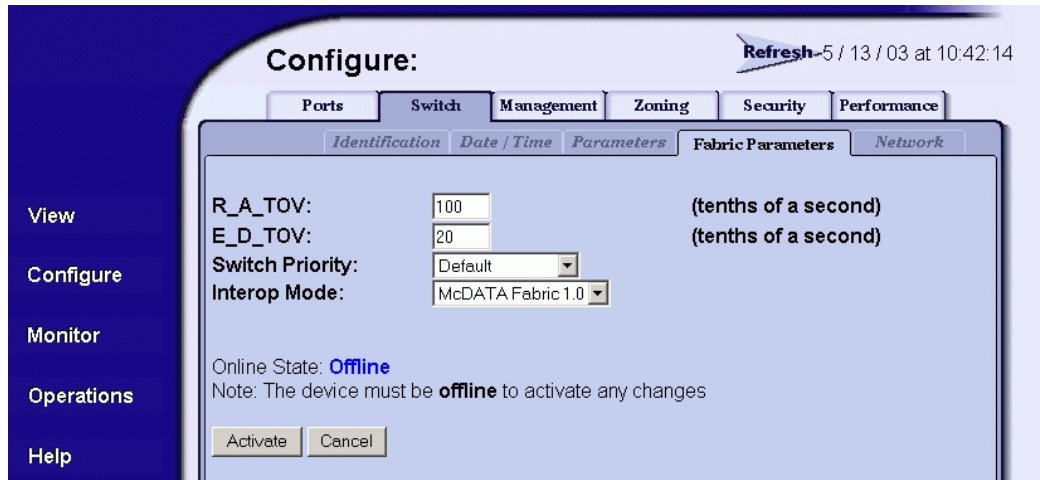


Figure 2-9 Configure Panel (Switch Page with Fabric Parameters Tab)

- a. At the *R_A_TOV* field, type a value between **10** through **1200** tenths of a second (one through 120 seconds). Ten seconds (**100**) is the recommended value.

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same *R_A_TOV* value. If the values are not identical, the *E_Port* connection to the element segments and the switch cannot communicate with the fabric. In addition, the *R_A_TOV* value must be greater than the *E_D_TOV* value.

- b. At the *E_D_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). Two seconds (**20**) is the recommended value.

NOTE: If the switch is attached to a fabric element, the switch and element must be set to the same *E_D_TOV* value. If the values are not identical, the *E_Port* connection to the element segments and the switch cannot communicate with the fabric. In addition, the *E_D_TOV* value must be less than the *R_A_TOV* value.

- c. Select from the *Switch Priority* drop-down list to set the switch priority. Available selections are *Default*, *Principal*, and *Never Principal*. The default setting is *Default*.

This value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest world wide name (WWN) becomes the principal switch.

At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all interswitch links (ISLs) segment.

- d. Select from the *Interop Mode* drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation. Available selections are:
 1. **McDATA Fabric 1.0** - Select this option if the switch is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
 - **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the switch is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs).

NOTE: When Open Fabric 1.0 is selected, the default zone is disabled, and you have to activate the default zone or enable the active zone set

2. Click *Activate* to save and activate the changes. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.
3. Set the switch online as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected

- b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

Configure Network Information

Verify the type of LAN installation with the customer's network administrator. If one switch is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change. Go to [Configure SNMP](#) on page 2-21.

If multiple switches are installed or a public LAN segment is used, network information must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a switch's IP address, subnet mask, or gateway address.

1. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
2. At the *Configure* panel, click the *Switch* tab, then click the *Network* tab. The *Switch* page displays with the *Network* tab selected ([Figure 2-10](#) on page 2-19).

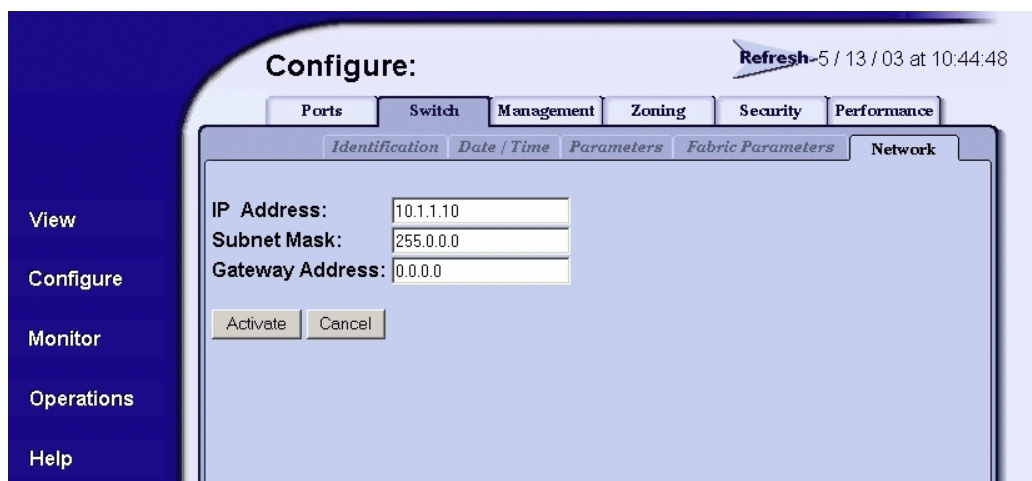


Figure 2-10 Configure Panel (Switch Page with Network Tab)

- a. At the *IP Address* field, type the new value as specified by the customer's network administrator (default is **10.1.1.10**).

- b. At the *Subnet Mask* field, type the new value as specified by the customer's network administrator (default is **255.0.0.0**).
 - c. At the *Gateway Address* field, type the new value as specified by the customer's network administrator (default is **0.0.0.0**).
3. Click *Activate* to save and activate the changes. The following message box displays (Figure 2-11).

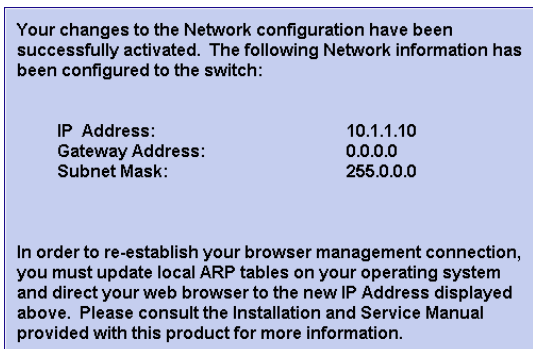


Figure 2-11 Network Information Message Box

- a. Select the *Exit* option from the *File* menu to close the SANpilot interface and browser applications. The Windows desktop displays.
 - b. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.
 - c. At the *Windows Workstation* menu, sequentially select the *Programs* and *Command Prompt* options. A disk operating system (DOS) window displays.
 - d. Delete the switch's *old* IP address from the ARP table. At the command (C:\) prompt, type **arp -d xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the old IP address for the switch.
 - e. Click close (X) at the upper right corner of the DOS window to close the window and return to the Windows desktop.
5. At the switch front panel, press and hold the **IML/RESET** button for ten seconds. The switch performs a power-on reset (POR).

6. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
7. At the browser, enter the switch's *new* IP address as the Internet URL. The *Enter Network Password* dialog box displays.
8. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

9. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed.

Configure SNMP

Perform this procedure to configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for up to six SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a switch event occurs. To configure SNMP trap recipients:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
2. At the *Configure* panel, click the *Management* tab. The *Management* page displays with the *SNMP* tab selected ([Figure 2-12](#)).

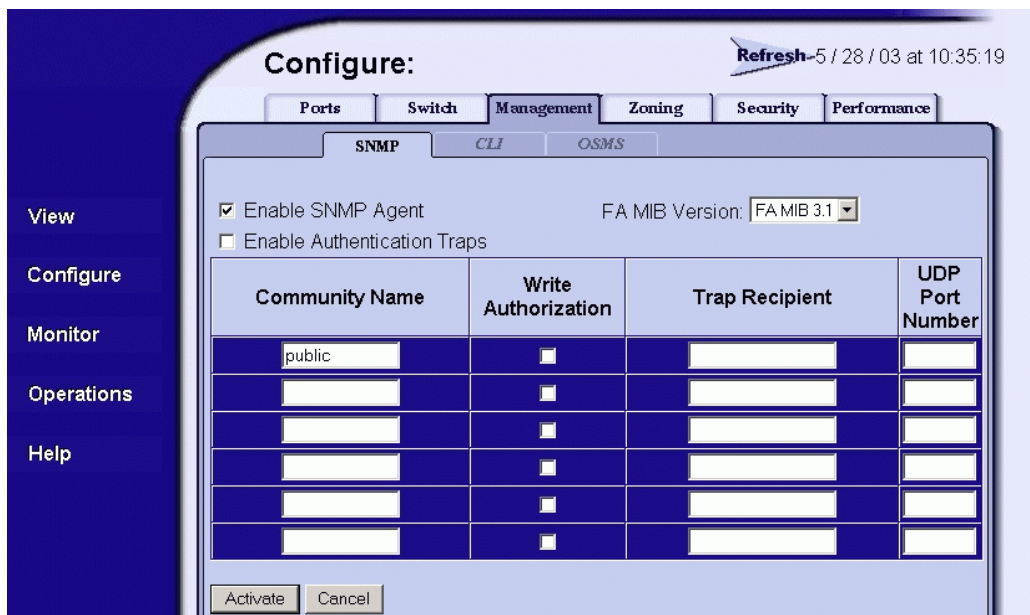


Figure 2-12 Configure Panel (Management Page with SNMP Tab)

- Click the *Enable SNMP Agent* check box to enable or disable the installed SNMP agent.
- Select the Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. This should be set to match the level of FA MIB used by the SNMP management stations that access the product. Available selections are:
 - FA MIB Version 3.0.**
 - FA MIB Version 3.1.**
- Click the *Enable Authentication Traps* check box to enable or disable transmission of SNMP trap messages to configured recipients.
- For each trap recipient to be configured, type a community name of 32 alphanumeric characters or less in the *Community Name* field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.

- e. Click the check box in the *Write Authorization* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.
 - f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field in four-byte, dotted-decimal format with a maximum of 16 characters. It is recommended the IP address be used.
 - g. The default UDP port number for trap recipients is **162**. Type a decimal port number in the *UDP Port Number* field to override the default value. The range for the UDP port number value is 1 to 65535.
3. Click *Activate* to save and activate the changes. The message **Your changes to the SNMP configuration have been successfully activated** appears.

Enable or Disable the CLI and SSH

Perform this procedure to toggle (enable or disable) the state of the director command line interface (CLI) as well as the configuration of the secure shell which is used to provide secure access and encrypted data when using the Telnet function.

1. At the *Configure* panel, click the *CLI* tab. The *Management* page displays with the *CLI* tab selected ([Figure 2-13](#)).

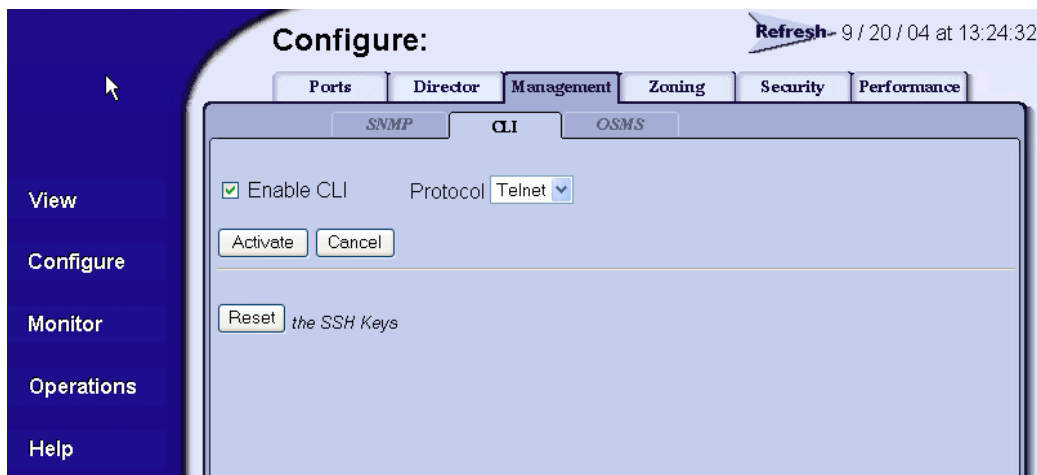


Figure 2-13 Configure Panel (Management Page with CLI Tab)

2. Perform one of the following steps as required:
 - Click *Enable* to activate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.
 - Click *Disable* to deactivate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.
3. To enable SSH, from the *Protocol* drop down box, select *SSH*.
4. Select *Activate* to enable SSH for Telnet.

NOTE: The default value is Telnet which means that data is not encrypted between the user and the product. By selecting SSH, data, such as a user ID and password, is encrypted between the user and the product.

Enable or Disable OSMS and Host Control

Perform this procedure to toggle (enable or disable) host control of the switch through the OSMS. The OSMS feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To enable or disable host control:

1. At the *Configure* panel, click the *OSMS* tab. The *Management* page displays with the *OSMS* tab selected (Figure 2-14).

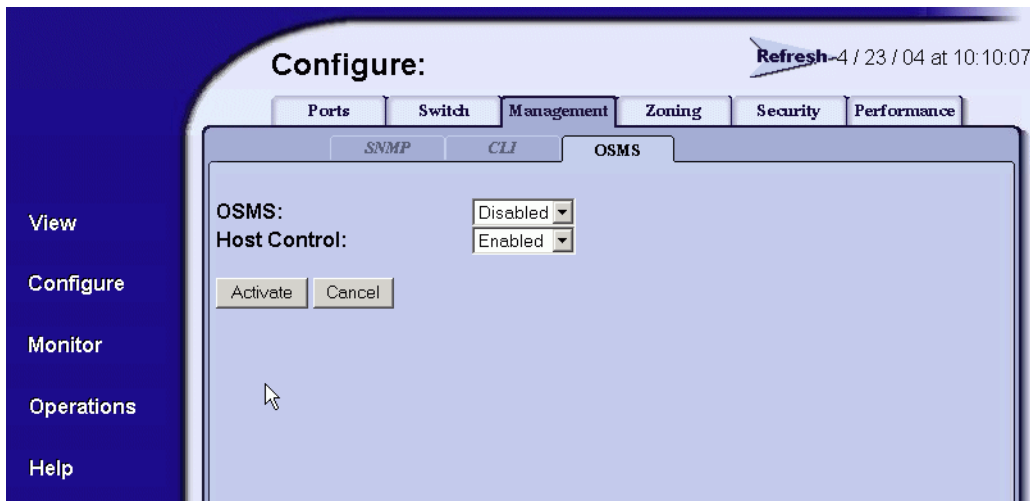


Figure 2-14 Configure Panel (Management Page with OSMS Tab)

2. Select either Enable or Disable from the drop-down box:
 - Select *Enable* to activate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.
 - Select *Disable* to deactivate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.
3. To change the host control state, select enable or disable from the drop-down box. Before you can enable host control state, OSMS must be enabled.

Change User Password

Perform this procedure to change the administrator-level and operator-level passwords used to access the SANpilot interface through the *Enter Network Password* dialog box.

1. At the *Configure* panel, click the *Security* tab. The *Security* page displays with the *Authorize Users* tab selected (Figure 2-15).

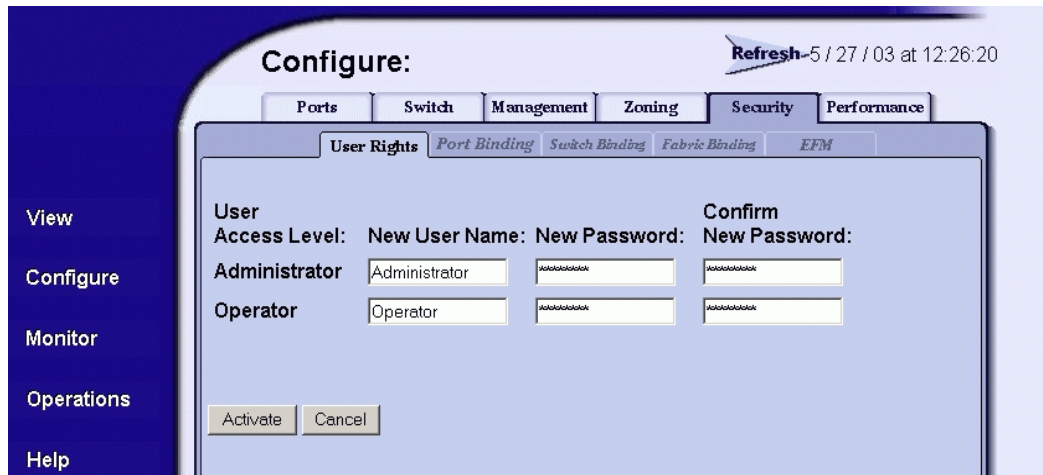


Figure 2-15 Configure Panel (Security Page with User Rights Tab)

2. Under the Currer User Records, enter the new password.
3. Click *Activate* to save the information. The message **Your changes to the user rights configuration have been successfully activated** appears.

NOTE: If you want to create a user account, review the SANpilot User's Guide for more information. Before you create a new user, you should review information on the security features provided with SANTegrity and RADIUS Servers such as authentication for the various interfaces such as Web (HTTP), CLI, Serial Port, E Port, N Port, and OSMS.

Configure Port Binding

Perform this procedure to configure Fibre Channel port binding by WWN. To configure port binding:

1. At the *Configure* panel, click the *Port Binding* tab. The *Security* page displays with the *Port Binding* tab selected (Figure 2-16).

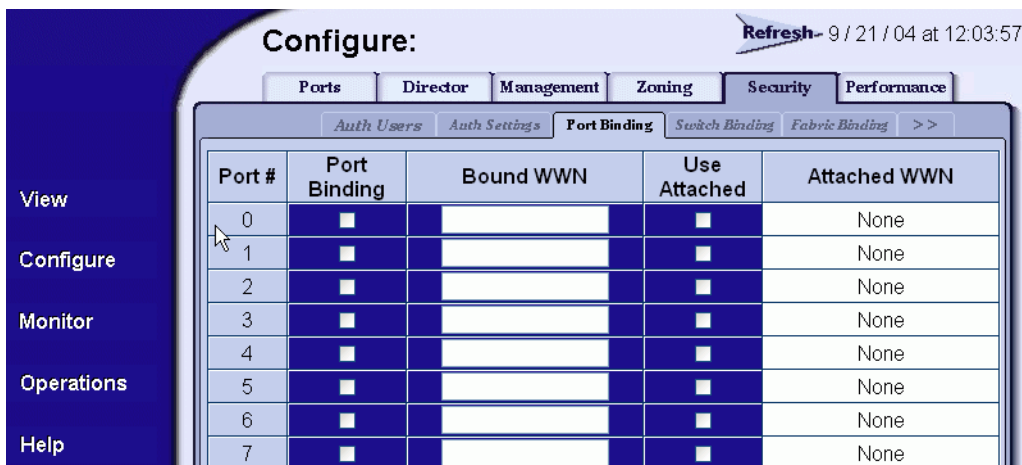


Figure 2-16 Configure Panel (Security Page with Port Binding Tab)

- a. Click the check box in the *Port Binding* column to enable or disable port binding for a specified port (default is disabled).
 - b. In the *Bound WWN* column, type the world wide name of the device to which the port is to be bound. If port binding is enabled, only the specified device can connect to the port. If port binding is enabled and no device is specified in the *Bound WWN* column, then no devices can connect to the port.
 - c. The *Attached WWN* column contains read-only fields that list the world wide names of attached Fibre Channel devices. Click the check box in the *Use Attached* column to indicate the world wide name specified in the *Attached WWN* column is to be used for port binding. After activation, the attached WWN appears in the *Bound WWN* column.
2. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.

Configure Switch Binding

Perform this procedure to configure switch binding by attached devices (nodes). The SANtegrity™ binding feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears.

Perform this procedure to configure switch binding by attached devices (nodes). The SANtegrity feature must be installed to access this control (*Install PFE Keys (Optional)* on page 2-38). If the feature is not installed, the message **This Feature Not Installed** appears.

Switch Binding functionality enables you to identify the devices with which the switch or director can communicate. Switch Binding is available only if the SANtegrity Binding feature is installed.

The *Switch Binding* tab view allows you to enable the product to communicate only with devices that are listed on the Switch Binding Membership List (SBML). Switch Binding restricts connections to only the devices listed on the SBML and allows no other devices to communicate with the switch. When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the event log. This provides security in environments that include a large number of devices by ensuring that only the specified set of devices are able to attach to a switch or director.

You can use the *Switch Binding* tab to enable Switch Binding and to create and change the SBML.

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features:

- Switch Binding can be enabled or disabled whether the product is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is offline you can disable Switch Binding, but this also disables Enterprise Fabric Mode.
- WWNs can be added to the SBML without regard to whether Switch Binding is enabled or disabled.
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the SBML.

To configure switch binding:

1. At the *Configure* panel, click the *Switch Binding* tab. The *Security* page displays with the *Switch Binding* tab selected ([Figure 2-17](#) on page 2-30).
2. Select the connection policy from the *Switch Binding State* drop-down list. The switch binding state indicates the type of binding restrictions imposed on the switch. Switch binding is enabled by activating Enterprise Fabric Mode (refer to [Enable or Disable Enterprise Fabric Mode](#) on page 2-34), or by enforcing a connection policy at the *Switch Binding State* drop-down list. Available selections are:
 - **Enable & Restrict E_Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through E_Ports.
 - **Enable & Restrict F_Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through F_Ports.
 - **Enable & Restrict All Ports** - Uses the switch binding membership list to restrict devices that can attach to the switch through any port.
 - **Disable Switch Binding** - Sets the switch binding state to disabled and removes restrictions on devices that can attach to the switch.



Figure 2-17 Configure Panel (Security Page with Switch Binding Tab)

3. Click *Submit*. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

NOTE: The **Disable Switch Binding** selection cannot be activated while Enterprise Fabric Mode is enabled and the switch is online.

4. The *Attached Nodes* drop-down list contains the world wide names of attached Fibre Channel devices. To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, perform one of the following:
 - Select a WWN from the *Attached Nodes* drop-down list and click the adjacent *Add Member* button.
 - Type a new WWN in the *Detached Node (WWN)* field and click the adjacent *Add Member* button.
5. To delete a device from the switch binding membership list, click the *Delete* button adjacent to the device WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the device.

Configuring the Switch Binding Membership List

The SBML contains the WWNs of devices that are allowed to communicate with the switch when Switch Binding is enabled. This list is configured using the *Switch Binding* tab.

The contents of the SBML are shown at the bottom of the tab, listed by WWN. The tab can show up to 64 list members. If the list contains more than 64 members, the other list members are shown on subsequent pages. To see the next page of list members, click the *Display More Members* option. To see the previous page of list members, click the *Display Previous Members* option. The message *All Members Displayed* appears on the last page of entries.

Adding a List Member

To add a new member to the SBML, perform the following procedure:

1. Select *Configure* from the navigation panel.
2. Select the *Security* tab and the *Switch Binding* tab.
3. Add the node to the list in one of the following ways:
 - Select an attached node from the *Attached Node WWN* drop down list.
 - If you select *Detached Node WWN*, type the WWN of a detached node. The WWN must be entered as hex digits, all uppercase, and with no colon separator between digits.
4. Select the *Add the following member by* button next to the node that you wish to add. The tab view refreshes and the node is now listed in the SBML at the bottom of the screen.
5. If a duplicate member is submitted for the membership list, an error message is displayed that an invalid membership list has been submitted.

Deleting a List Member

WWNs can only be removed from the SBML if any of the following are true:

- The director or switch is offline.
- Switch Binding is disabled.
- The switch or device with the WWN is not currently connected to the director or switch (detached node).
- Switch Binding is not enabled for the same port type as enabled for the connection policy. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding connection policy is set to *Enabled & Restrict F_Ports*.

- The switch or device with the WWN is connected to a port that is blocked.

To delete a member or all members from the SBML, perform the following procedure:

1. Select *Configure* from the navigation panel.
2. Select the *Security* tab and the *Switch Binding* tab.
3. Select the *Delete* button next to the listing for the member.
4. At the *Are you sure you want to delete this member?* prompt, click OK. The SBML redisplay without the deleted member.
5. If you want to delete all of the members of a switch binding membership list, select *Delete All Members from the Switch Binding Membership List*.

Configure Fabric Binding

Perform this procedure to configure fabric binding by attached fabric member (domain ID and WWN). The SANtegrity binding feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To configure fabric binding:

1. At the *Configure* panel, click the *Fabric Binding* tab. The *Security* page displays with the *Fabric Binding* tab selected ([Figure 2-18](#)).

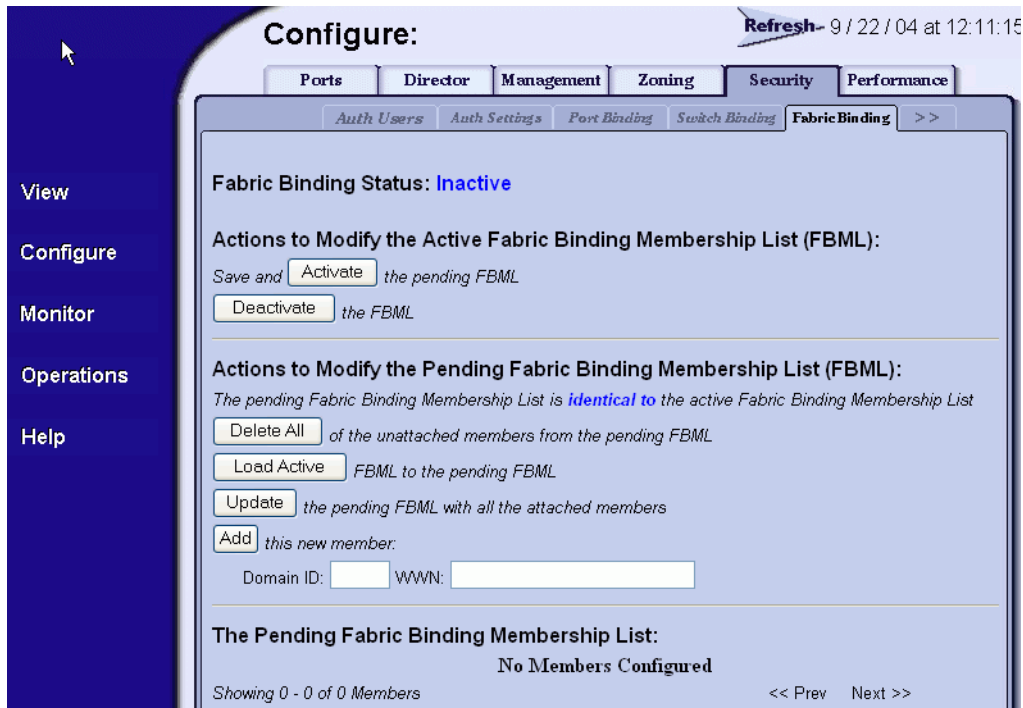


Figure 2-18 Configure Panel (Security Page with Fabric Binding Tab)

2. The Fabric Binding tab is divided into sections by the following headings. Configure fabric binding from the following:
 - Fabric Binding Status—Identifies whether Fabric Binding is active or inactive on the product.
 - Actions to Modify the Active Fabric Binding Membership List (FBML)—Enables you to activate and deactivate Fabric Binding using the following buttons:
 - Activate: By selecting this button, you save the pending FBML as the active FBML and activate Fabric Binding.
 - Deactivate: By selecting this button, you change the Fabric Binding status from active to inactive, disabling Fabric Binding.
 - Actions to Modify the Pending Fabric Binding Membership List (FBML)—Enables you to modify the pending FBML using the following buttons:

- Delete All: By selecting this button, you can delete all members from the pending FBML that are not attached to the current fabric. Members that are attached must remain in the list, because the membership list must contain all attached members to be activated.
- Load Active: By selecting this button, you can copy the contents of the active FBML to the pending FBML. The added members may include unattached members of the active FBML.
- Update: By selecting this button, you can update the pending FBML to include all currently attached fabric members. Unattached members of the active FBML are not added to the list by this action.
- Add: By selecting this button, you can add a new member to the FBML as defined in the *Domain ID* and *WWN* fields below the button.
 - The Pending Fabric Binding Membership List—Enables you to view the pending FBML as it is being updated and to delete unattached members from the list. Members of the pending FBML are listed by WWN.

NOTE: For detailed instructions on configuring fabric binding, review the *SANpilot User Manual*.

Enable or Disable Enterprise Fabric Mode

Perform this procedure to toggle (enable or disable) the use of Enterprise Fabric Mode (EFM). The SANtegrity binding feature must be installed to access this control. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To enable or disable EFM:

1. At the *Configure* panel, click the *EFM* tab. The *Security* page displays with the *EFM* tab selected ([Figure 2-19](#)).

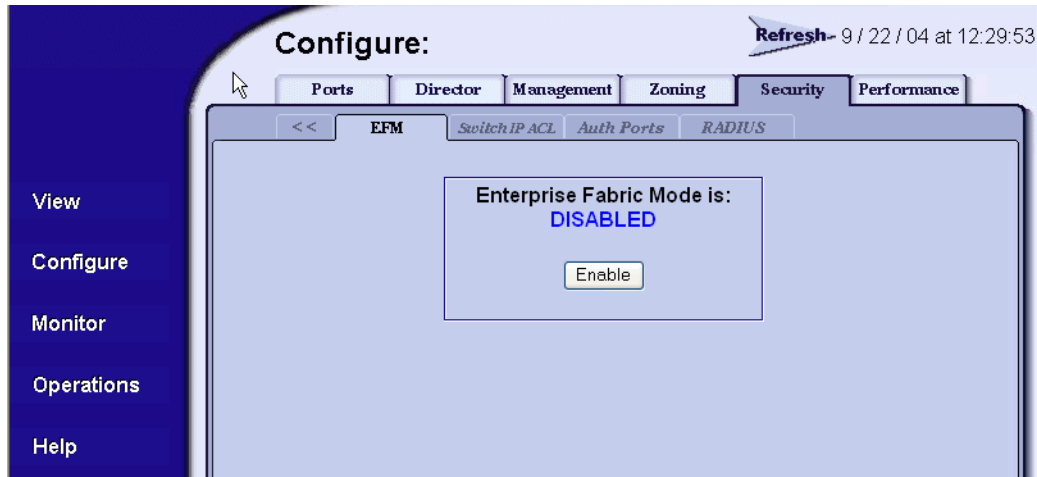


Figure 2-19 Configure Panel (Security Page with EFM Tab)

2. Perform one of the following steps as required:
 - Click *Enable* to activate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.
 - Click *Disable* to deactivate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.

NOTE: For detailed information on configuring Enterprise Fabric Mode, review the *SANpilot User Manual*.

Configure OpenTrunking

Perform this procedure to configure OpenTrunking parameters. The OpenTrunking feature must be installed to access this control. Refer to *Install PFE Keys (Optional)* on page 2-38 for instructions. If the feature is not installed, the message **This Feature Not Installed** appears. To configure OpenTrunking parameters:

1. At the *Configure* panel, click the *Performance* tab. The *Performance* page displays with the *OpenTrunking* tab selected (Figure 2-20 on page 2-36).

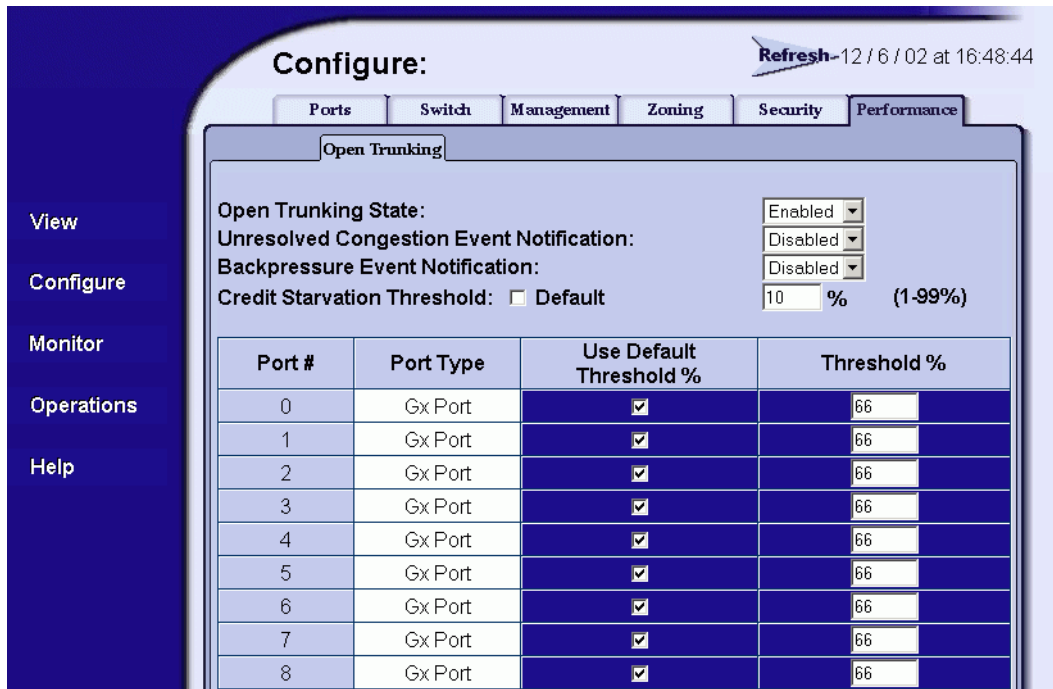


Figure 2-20 Configure Panel (Performance Page with OpenTrunking Tab)

- At the *OpenTrunking State* field, select *Enabled* or *Disabled*. When this parameter is enabled, the optional OpenTrunking feature is functional.
- At the *Unresolved Congestion Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, unresolved congestion events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

An unresolved congestion event occurs for a low-BB_Credit ISL when the switch's firmware rerouting algorithm cannot route data flow to an alternate path (because doing so would exceed the alternate path's low BB_Credit threshold).

- At the *Backpressure Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, backpressure events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

A backpressure event occurs when the percent time an ISL has low BB_Credit exceeds the low BB_Credit threshold.

- d. The low BB_Credit threshold is the percent time an ISL is allowed to not transmit data because BB_Credit is unavailable. When the threshold is exceeded, data is rerouted to another ISL. In addition, traffic cannot be rerouted to another low-threshold ISL. Use one of the following to set the low BB_Credit threshold:
 - Click the *Default* check box. A check mark appears in the box and a calculated default value appears (1% to 99%) in the *Low BB_Credit Threshold* field. If the default value is enabled, a value cannot be entered in the *Low BB_Credit Threshold* field.
 - Ensure the *Default* check box is blank. At the *Low BB_Credit Threshold* field, type a percentage value from 1% to 99%.

NOTE: The default low BB_Credit threshold is calculated by the switch's firmware and performs well in most cases.

2. For each switch port:
 - a. Click the check box in the *Default Threshold %* column. A check mark appears in the box and a calculated default value appears (1% to 99%) in the associated field in the *Threshold %* column. If the default value is enabled, a value cannot be entered in the *Threshold %* column.
 - b. Ensure the check box in the *Default Threshold %* column is blank. At the associated field in the *Threshold %* column, type a percentage value from 1% to 99%.

NOTE: The default low BB_Credit threshold is calculated by the switch's firmware and performs well in most cases.

3. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.
4. If additional optional features are to be installed, go to [Install PFE Keys \(Optional\)](#) below. If no PFE keys are to be installed, go to [Task 4: Configure Switch Network Information \(Optional\)](#) on page 2-39.

Install PFE Keys (Optional)

Perform this procedure to install optional features. After purchasing a feature, obtain the required product feature enablement (PFE) key by following the enclosed instructions. A PFE key is an alphanumeric string consisting of both uppercase and lowercase characters. The total number of characters may vary. The key is case sensitive and must be entered exactly, including dashes. The following is an example of a PFE key format:

XxXx-XXxX-xxXX-xX.

After obtaining the PFE key, install the feature as follows:

1. Set the switch offline as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
3. Click the *Feature Installation* tab. The *Operations* panel opens with the *Feature Installation* page displayed (Figure 2-21).

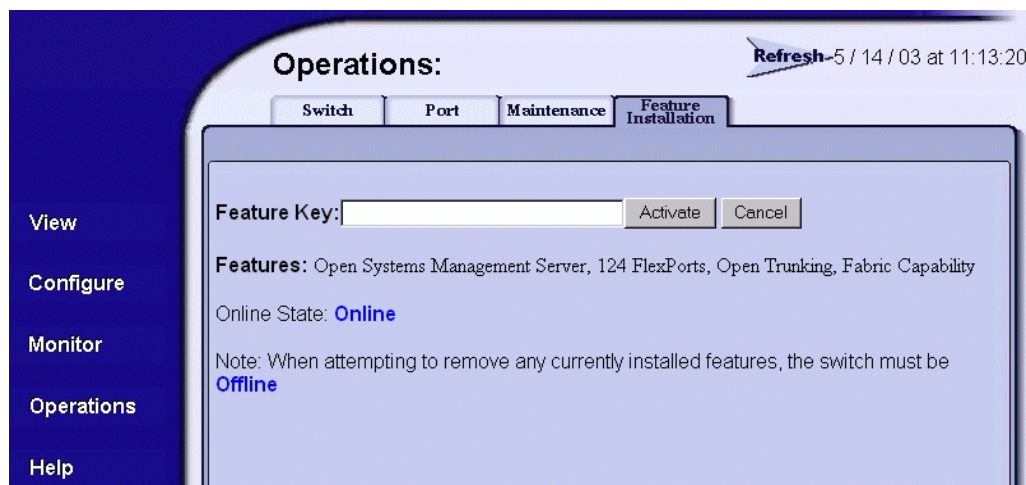


Figure 2-21 Operations Panel (Feature Installation Tab)

4. Type the PFE key and click *Activate*. The interface displays a confirmation page with a warning, stating this action overrides the current set of switch features.
5. Click *Activate* to activate the new PFE key. The switch performs an IPL when the key is activated.

NOTE: When *Activate* is selected, all current features are replaced with new features. Features not included in the new feature key are no longer available on the system. Because of this, it is important to verify that the feature key enables all of designed features.

6. Set the switch online as follows:
 - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
 - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

NOTE: PFE keys are encoded to work with the serial number of the installed switch only. Record the key to re-install the feature if required. If the switch fails and must be replaced, obtain new PFE keys from the McDATA Solution Center (800-752-4572 or support@mcddata.com). Please have the serial numbers of the failed and replacement switches, and the old PFE key number or transaction code.

7. Go to [Task 4: Configure Switch Network Information \(Optional\)](#) below.

Task 4: Configure Switch Network Information (Optional)

The switch is delivered with default network addresses as follows:

- **MAC address** - The media access control (MAC) address is programmed into FLASH memory on the control processor (CTP) card at the time of manufacture. The MAC address is unique for each switch, and should not be changed.
- **IP address** - The default IP address is **10.1.1.10**. If multiple switches are installed on the same LAN, each switch must have a unique IP address. One switch can use the default address, but the addresses of the remaining switches must be changed.

NOTE: If multiple switches are delivered in a McDATA Fabriccenter equipment cabinet, all devices are configured with unique IP addresses that do not require change. The addresses require change only if multiple equipment cabinets are LAN-connected.

- **Subnet mask** - The default subnet mask is **255.0.0.0**. If the switch is installed on a complex public LAN with one or more routers, the address may require change.
- **Gateway address** - The default gateway address is **0.0.0.0**. If the switch is installed on a dedicated LAN with no connection through a router, the address does not require change. If the switch is installed on a public LAN (corporate intranet), the gateway address must be changed to the address of the corporate intranet's local router.

Verify the type of LAN installation with the customer's network administrator. If multiple switches are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme. The following tools are provided with the switch or by installation or service personnel and are required to perform this task:

- A maintenance terminal (desktop or notebook PC) with:
 - The Microsoft Windows 98, Windows 2000, Windows ME, Windows XP, or Windows NT 4.0 operating system.
 - RS-232 serial communication software (such as ProComm Plus or HyperTerminal). HyperTerminal is provided with the Windows operating systems.
- An asynchronous RS-232 modem cable.

Perform the following steps to change a switch's IP address, subnet mask, or gateway address.

1. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the switch chassis. Connect one end of the RS-232 modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays. If required, refer to operating instructions shipped with the PC.

4. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

NOTE: The following steps describe changing network addresses using HyperTerminal serial communication software.

5. At the *Windows Workstation* menu, sequentially select the *Programs* option, *Accessories* option, *Hyperterminal* option, and *HyperTerminal* option. The *Connection Description* dialog box displays (Figure 2-22 on page 2-41).

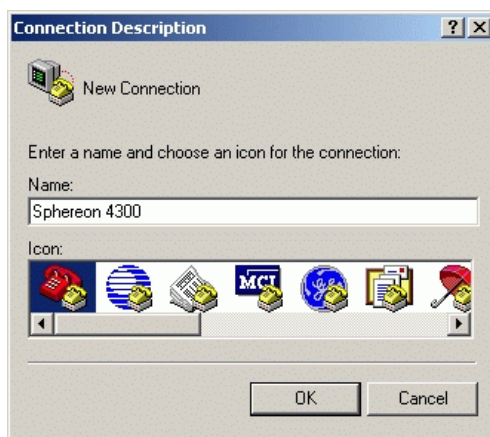


Figure 2-22 Connection Description Dialog Box

6. Type **Sphereon 4300** in the *Name* field and click *OK*. The *Connect To* dialog box displays (Figure 2-23).



Figure 2-23 Connect To Dialog Box

7. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click OK. The *COMn Properties* dialog box displays, where *n* is 1 or 2 (Figure 2-24 on page 2-42).

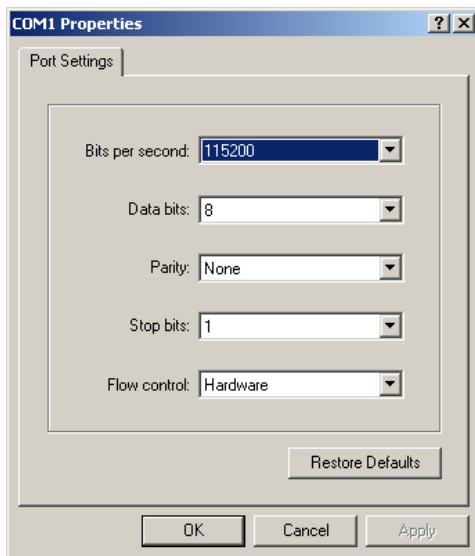


Figure 2-24 COMn Properties Dialog Box

8. Configure the *Port Settings* parameters as follows:

- *Bits per second* - **115200**.
- *Data bits* - **8**.
- *Parity* - **None**.
- *Stop bits* - **1**.
- *Flow control* - **Hardware** or **None**.

When the parameters are set, click OK. The *Sphereon 4300 - HyperTerminal* window displays.

9. At the **>** prompt, type the user-level password (the default is **password**) and press **Enter**. The password is case sensitive. The *Sphereon 4300 - HyperTerminal* window (Figure 2-25 on page 2-43) displays with software and hardware version information for the switch, and a **C >** prompt at the bottom of the window.

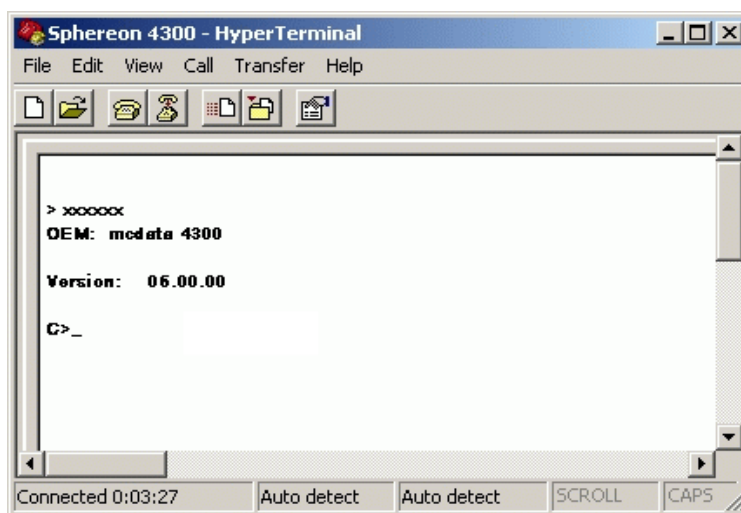


Figure 2-25 Sphereon 4300 - HyperTerminal Window

10. At the **C >** prompt, type the **ipconfig** command and press the **Enter** key. The *Sphereon 4300 - HyperTerminal* window displays with configuration information listed as follows:
 - *MAC Address*.
 - *IP Address* (default is **10.1.1.10**).

- *Subnet Mask* (default is **255.0.0.0**).
- *Gateway Address* (default is **0.0.0.0**).
- *Auto Negotiate*.
- *Speed*.
- *Duplex*.

Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.

11. Change the IP address, subnet mask, and gateway address as directed by the customer's network administrator. To change the switch network addresses, type the following at the **C >** prompt and press the **Enter** key.

```
ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz
```

The IP address is always *xxx.xxx.xxx.xxx*, the subnet mask is always *yyy.yyy.yyy.yyy*, and the gateway address is always *zzz.zzz.zzz.zzz*, where the octets *xxx*, *yyy*, and *zzz* are decimals from zero through 255. If a network address is to remain unchanged, type the current address in the respective field.

When the new network addresses are configured at the switch, the message **Request completed OK** displays at the bottom of the *Sphereon 4300 - HyperTerminal* window.

12. Select the *Exit* option from the *File* pull-down menu to close the HyperTerminal application. A HyperTerminal message box appears (Figure 2-26):

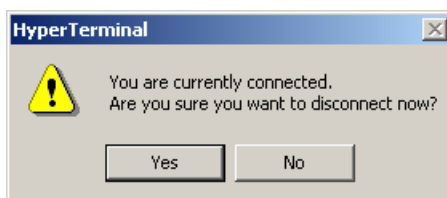


Figure 2-26 HyperTerminal Dialog Box (1)

13. Click **Yes**. A second HyperTerminal message box appears (Figure 2-27):

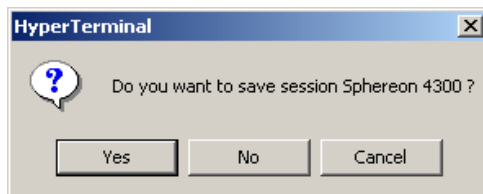


Figure 2-27 HyperTerminal Dialog Box (2)

14. Click *No* to exit and close the HyperTerminal application.
15. Power off the maintenance terminal:
 - a. Click *Start* at the left side of the task bar and select the *Shut Down* option. The *Shut Down Windows* dialog box appears.
 - b. At the *Shut Down Windows* dialog box, select the *Shut down* option from the list box and click *OK* to power off the PC.
16. Disconnect the RS-232 modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.
17. At the switch front panel, press and hold the **IML/RESET** button for ten seconds. The switch performs a POR.
18. Connect the switch to the customer-supplied Ethernet LAN segment. To connect the switch:
 - a. Connect one end of the Ethernet patch cable (supplied with the switch) to the RJ-45 connector (labelled **10/100**) on the left front of the switch chassis.
 - b. Connect the remaining end of the Ethernet cable to the LAN as directed by the customer's network administrator.

Task 5: Cable Fibre Channel Ports

Perform this task to connect devices to the switch. To cable Fibre Channel ports:

1. Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric switches to ports at the front of the switch.

2. Connect device cables to SFP optical port transceivers. Start with port 0 (far right) and continue sequentially to the left through port 11.
3. Perform one of the following:
 - If the switch is installed on a table or desk top, bundle and secure the Fibre Channel cables as directed by the customer.
 - If the switch is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them as directed by the customer.
 - If the switch is installed in a McDATA Fabriccenter equipment cabinet, bundle Fibre Channel cables from the switch and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.

Task 6: Configure Zoning (Optional)

Perform this procedure to:

- Configure, change, add, or delete zones. A zone is a group of devices that can access each other through port- to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.
- Configure, change, enable, or disable zone sets. A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time.

Configure Zones

To configure zones at the SANpilot interface:

1. At the *Configure* panel, click the *Zoning* tab. The *Zoning* page displays with the *Zone Set* tab selected. Click the *Zones* tab. The *Zoning* page displays with the *Zones* tab selected ([Figure 2-28](#)).

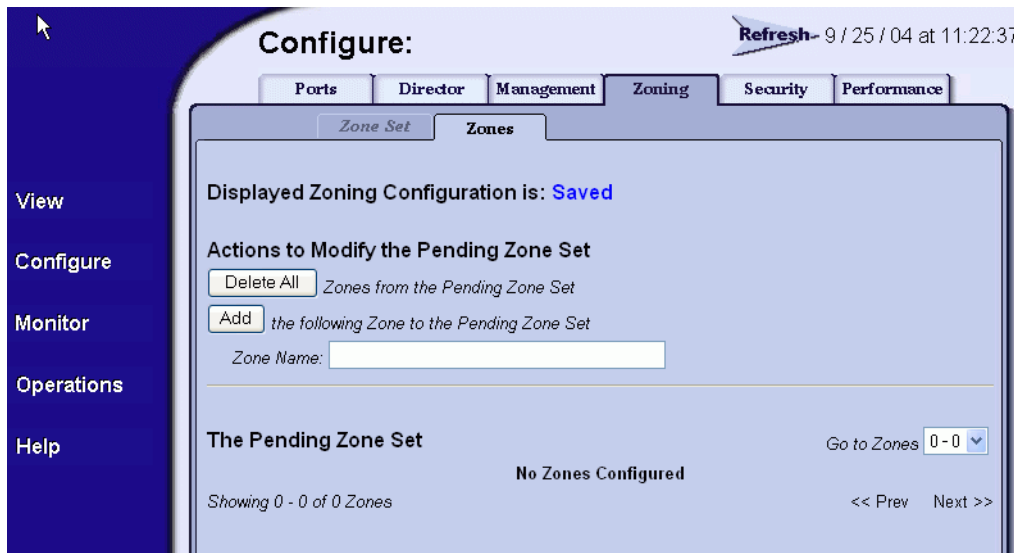


Figure 2-28 Configure Panel (Zoning Page with Zones Tab)

2. To configure a zone, first add the zone name to the zoning library. The following naming conventions apply to zones and zone sets:
 - All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
 - The first character of a zone set name must be a letter (A through Z or a through z).
 - A zone set name cannot contain spaces.
 - Valid characters are alphanumeric and the caret (^), hyphen (-), underscore (_), or dollar (\$) symbols.
 - A zone set name can have a maximum of 64 characters.
3. Type the zone name and click *Add New Zone*. After the name is validated, the new zone name (**Zone-1**) and an associated *Delete* button appear at the bottom of the page. Note the following:
 - **Save and activate the zone** - Changes to a zone or zoning configuration are not saved and activated on the switch until saved as part of a zone set. Go to [Configure Zone Sets](#) on page 2-49 to perform this function.

- **Delete all zones** - To delete all configured zones and zone members, click *Delete All Zones*. A confirmation dialog box displays. Click OK to delete all zones.
 - **Delete a single zone** - To delete a single zone and its zone members, click the *Delete* button adjacent to the zone name. A confirmation dialog box displays. Click OK to delete the zone.
 - **Go to zones**- If a zone set contains more than 64 zones, the *Go to zones* link activates to display subsequent pages. In addition, the *Go to zones* link activates on subsequent displayed pages.
4. To add devices (members) to the zone, click the zone name (**Zone-1**). The *Zoning* page displays with the *Modify Zone* tab selected (Figure 2-29 on page 2-48).

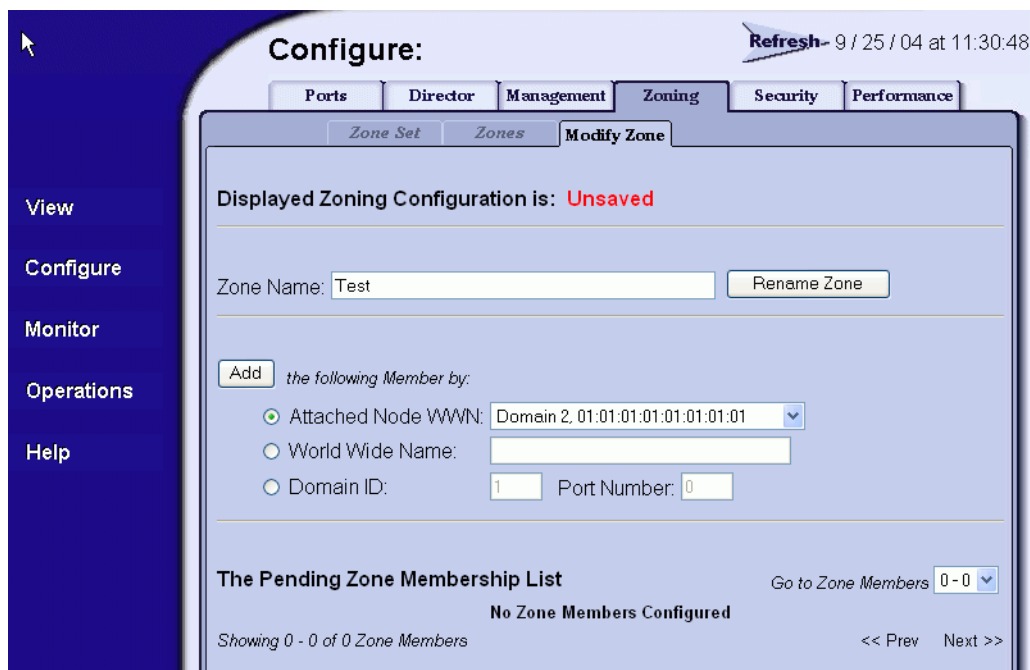


Figure 2-29 Configure Panel (Zoning Page with Modify Zone Tab)

5. To rename a configured zone, type the new name in the *Zone* field and click *Rename Zone*. After the name is validated, the zone name is changed.
6. Add or delete zone members as follows:

- **Add member by attached node WWN** - Select the WWN of an attached device (node) from the *Attached Node World Wide Name* drop-down list and click the adjacent *Add Member* button. The device is added to the zone.
 - **Add member by WWN** - Type the WWN of an attached device in the *World Wide Name* field and click the adjacent *Add Member* button. The device is added to the zone.
 - **Add member by domain ID and port number** - Type the domain ID (**1** through **31**) of the switch in the *Domain ID* field, type the switch port number (**0** through **11**) to which a device is attached, and click the adjacent *Add Member* button. The device attached to that port is added to the zone.
7. Changes to a zone, zoning configuration, or zone member are not saved and activated on the switch until saved as part of a zone set. Go to [Configure Zone Sets](#) below to perform this function.

Configure Zone Sets

To configure zone sets at the SANpilot interface:

1. At the *Configure* panel and *Zoning* page, click the *Zone Set* tab. The *Zoning* page displays with the *Zone Set* tab selected ([Figure 2-30](#)).

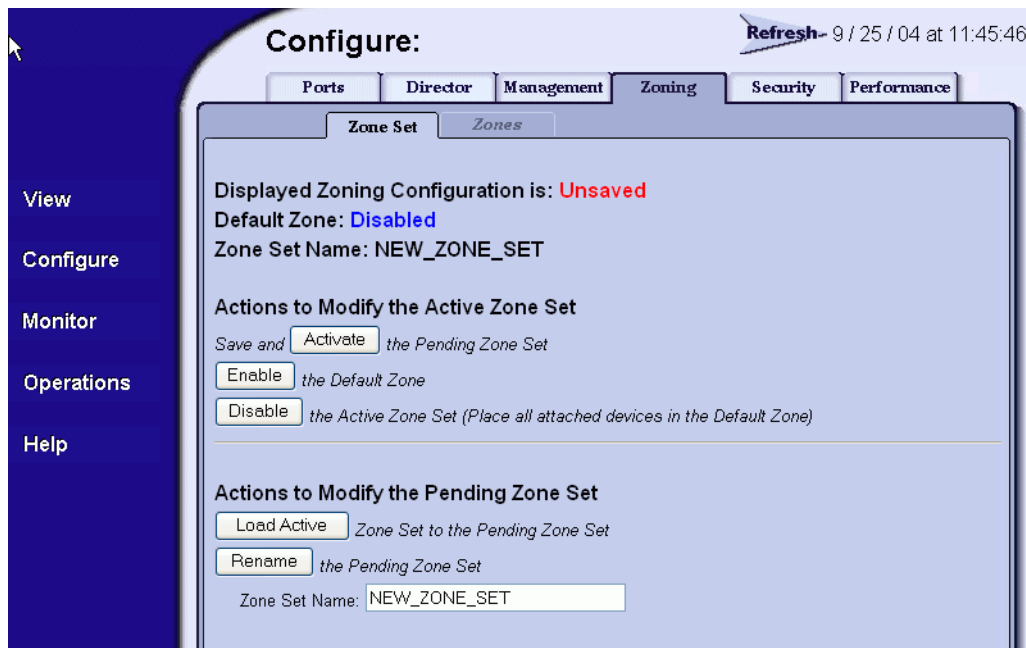


Figure 2-30 Configure Panel (Zoning Page with Zone Set Tab)

2. To create a zone set that incorporates zones and zone members (configured under [Configure Zones](#) on page 2-46), type a new zone set name in the *Zone Set Name* field.
3. Click *Save and Activate Zoning Configuration*. After the zone set name is validated, a confirmation dialog box displays.
4. Click OK to save and activate the new zone set. The message **Your changes to the Zoning configuration have been successfully activated** appears. Note the following:
 - **Rename pending zone set** - To rename a zone set, type the new name in the *Zone Set Name* field. Click *Rename Pending Zone Set*. The new zone set name is validated and changed.
 - **Enable or disable default zone** - To toggle (enable or disable) the default zone state, click *Enable Default Zone* or *Disable Default Zone*. Depending on the toggle state, the *Default Zone* field changes to **Enabled** or **Disabled**.

- **Disable zone set** - To disable the active zone set and place all attached devices in the default zone, click *Disable Zone Set*. A confirmation dialog box displays. Click OK to disable the active zone set.
- **Discard changes** - To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click *Discard Changes*. A confirmation dialog box displays. Click OK to discard the changes.

Task 7: Connect Switch to a Fabric Element (Optional)

To provide fabric-attached Fibre channel connectivity for devices connected to the Sphereon 4300 Switch, connect the switch to an expansion port (E_Port) of a fabric element (switch or director). Any switch can be used to form this ISL. To connect the Sphereon 4300 Switch to a fabric element and create an ISL:

1. Ensure the fabric element is accessible by the SANpilot interface. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.
2. Ensure the preferred domain ID for the Sphereon 4300 Switch is unique and does not conflict with the ID of another switch or director participating in the fabric. Refer to [Task 3: Configure the Switch at the SANpilot Interface](#) on page 2-6.
3. Ensure the R_A_TOV and E_D_TOV values for the Sphereon 4300 Switch are identical to the values for all switches or directors participating in the fabric. Refer to [Task 3: Configure the Switch at the SANpilot Interface](#).
4. Route a multimode or singlemode fiber-optic cable (depending on the type of transceiver installed) from a customer-specified E_Port of the fabric element to the front of the switch.
5. Connect the director-attached fiber-optic cable to a Sphereon 4300 Switch port as directed by the customer.
6. At the *Configure* panel, select the *View* option at the left side of the panel. The *View* panel opens with the *Switch* page displayed.
7. Double-click the graphical port connector used for the fabric ISL (connected in [step 5](#)).
8. The *View* panel opens with the *Port Properties* page displayed. Port properties appear for the selected port.

9. Ensure the *Operational State* field displays **Online** and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

Task 8: Register with the McDATA File Center

To complete the installation, register with the McDATA File Center web site to receive e-mail updates and access the following:

- Technical publications.
- Firmware and software upgrades.
- Technical newsletters.
- Release notes.

To register with the McDATA File Center:

1. At a PC with Internet access, open the McDATA File Center home page ([Figure 2-31](#) on page 2-52). The uniform resource locator (URL) is <http://central.mcddata.com>.

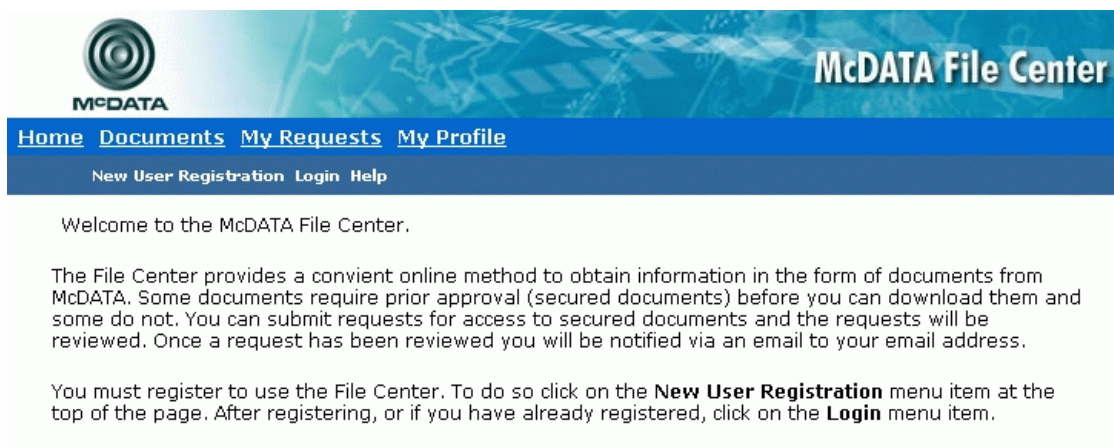


Figure 2-31 McDATA File Center Home Page

2. Select (click) the *New User Registration* option at the top of the home page. The File Center's *New User Registration* page displays ([Figure 2-32](#) on page 2-54). Use the registration page to input required and optional user information.

The following information is required:

- Password.
 - Verify password.
 - First name.
 - Last name.
 - E-mail address.
 - Company.
 - Title.
3. Complete the information fields as required and click *Register*. The registration is complete and File Center login information is transmitted to the e-mail address specified on the *New User Registration* page.
 4. At the browser PC, close the Internet session. If no switch problems are indicated, installation tasks are complete.

[Home](#) [Documents](#) [My Requests](#) [My Profile](#)

New User Registration [Login](#) [Help](#)

Registration: New File Center

Below are a few fields we need you to fill in so that we can better fulfill your request for information. You will only have to do this once and the information will not be released to any other companies. Information requested below will assist us in routing your request to the appropriate SAN Professional.

There are some mandatory fields that have not been filled in yet or are invalid. Please correct them and click the Register button. Field specific errors are shown to the right of the fields.

Basic User Information

In this section we need to collect some basic information about you and how we can contact you.

Password:	<input type="password"/>	Password is required.
Verify Password:	<input type="password"/>	Verify Password is required.
First Name:	<input type="text"/>	First Name is required.
Middle Name:	<input type="text"/>	
Last Name:	<input type="text"/>	Last Name is required.
E-mail Address:	<input type="text"/>	E-mail Address is required.
Company:	<input type="text"/>	Company is required.
Title:	<input type="text"/>	Title is required.
Phone Number:	<input type="text"/>	
Fax Number:	<input type="text"/>	

Register

Figure 2-32 McDATA File Center (New User Registration Page)

This chapter describes diagnostic procedures used by service representatives to fault isolate Sphereon 4300 Switch problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

Fault isolation and related service procedures are provided through MAPs. The procedures vary depending on the diagnostic information provided. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system events, isolate a switch failure, repair the failure, and verify switch operation.

Factory Defaults

[Table 3-1](#) on page 3-2 lists factory-set defaults for Sphereon 4300 Switch passwords (customer and maintenance-level), and the switch's Internet Protocol (IP) address, subnet mask, and gateway address.

Table 3-1 Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick Start

[Table 3-2](#) lists and summarizes the MAPs. Fault isolation normally begins at [MAP 0000: Start MAP](#) on page 3-6.

Table 3-2 MAP Summary

MAP	Page
MAP 0000: Start MAP	3-6
MAP 0100: Power Distribution Analysis	3-18
MAP 0200: POST Failure Analysis	3-21
MAP 0300: Loss of Web Browser PC Communication	3-23
MAP 0400: FRU Failure Analysis	3-30
MAP 0500: Port Failure and Link Incident Analysis	3-35
MAP 0600: Fabric, ISL, and Segmented Port Problem Determination	3-54

[Table 3-3](#) on page 3-3 lists event codes and the corresponding MAP references. The table provides a quick start guide if an event code is readily available.

Table 3-3 Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0600 .
021	Name Server database invalid.	Go to MAP 0600 .
031	SNMP request received from unauthorized community.	Add a community name through the SANpilot interface.
051	Management Server database invalid.	Go to MAP 0600 .
052	Management Server internal error.	Go to MAP 0600 .
061	Fabric Controller database invalid.	Go to MAP 0600 .
062	Maximum interswitch hop count exceeded.	Go to MAP 0600 .
063	Remote switch has too many ISLs.	Go to MAP 0600 .
070	E_Port is segmented.	Go to MAP 0600 .
071	Switch is isolated.	Go to MAP 0600 .
072	E_Port connected to unsupported switch.	Go to MAP 0600 .
073	Fabric initialization error.	Go to Collect Maintenance Data on page 4-22.
074	ILS frame delivery error threshold exceeded.	Go to Collect Maintenance Data on page 4-22.
080	Unauthorized worldwide name.	Go to MAP 0500 .
081	Invalid attachment.	Go to MAP 0500 .
120	Error detected while processing system management command.	Go to Collect Maintenance Data on page 4-22.
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to MAP 0600 .
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0600 .

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
143	Low BB_Credit relieved on an ISL.	No action required.
150	Zone merge failure.	Go to MAP 0600 .
151	Fabric configuration failure.	Go to Collect Maintenance Data on page 4-22.
300	Cooling fan propeller failed.	Go to MAP 0400 .
301	Cooling fan propeller failed.	Go to MAP 0400 .
302	Cooling fan propeller failed.	Go to MAP 0400 .
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200 .
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200 .
412	CTP watchdog timer reset.	Go to Collect Maintenance Data on page 4-22.
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0400 .
433	Non-recoverable Ethernet fault.	Go to MAP 0400 .
440	Embedded port hardware failed.	Go to MAP 0400 .
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0500 .
507	Loopback diagnostics port failure.	Go to MAP 0500 .
508	Fibre Channel port anomaly detected.	No action required.

Table 3-3 Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to MAP 0500 .
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0500 .
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0500 .
582	Bit error threshold exceeded.	Go to MAP 0500 .
583	Loss of signal or loss of synchronization.	Go to MAP 0500 .
584	Not operational primitive sequence received.	Go to MAP 0500 .
585	Primitive sequence timeout.	Go to MAP 0500 .
586	Invalid primitive sequence received for current link state.	Go to MAP 0500 .
810	High temperature warning (CTP thermal sensor).	Go to MAP 0400 .
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0400 .

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Sphereon 4300 Switch. Fault isolation begins at the Internet-connected PC accessing the SANpilot interface, failed switch, or switch-attached host.

1

Prior to fault isolation, acquire the following from the customer:

- A system configuration drawing or planning worksheet that includes the customer-supplied web browser PC accessing the SANpilot interface, switch, other McDATA products, and device connections.
- The location of the web browser PC and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- The administrator user name and password of the customer-supplied server accessing the SANpilot interface. Both are case sensitive and required when prompted at the *Username and Password Required* dialog box.

Continue to the next step.

2

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer), an Internet connection to the switch reporting the problem, and communicating with the switch through the SANpilot interface?

YES NO



Go to [step 19](#).

3

Is the web-browser PC powered on and communicating with the switch through the Internet connection and SANpilot interface?

NO YES



Go to [step 5](#).

4

Boot the web-browser PC.

- a. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.
- b. Launch the PC browser application by double-clicking the Netscape Navigator or Internet Explorer icon at the Windows desktop.
- c. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [step 1](#)). The *Username and Password Required* dialog box appears ([Figure 3-1](#)).



Figure 3-1 Username and Password Required Dialog Box

- d. Type the user name and password obtained in [step 1](#) and click **OK**. The SANpilot interface opens with the *View* panel displayed ([Figure 3-2](#) on page 3-8).

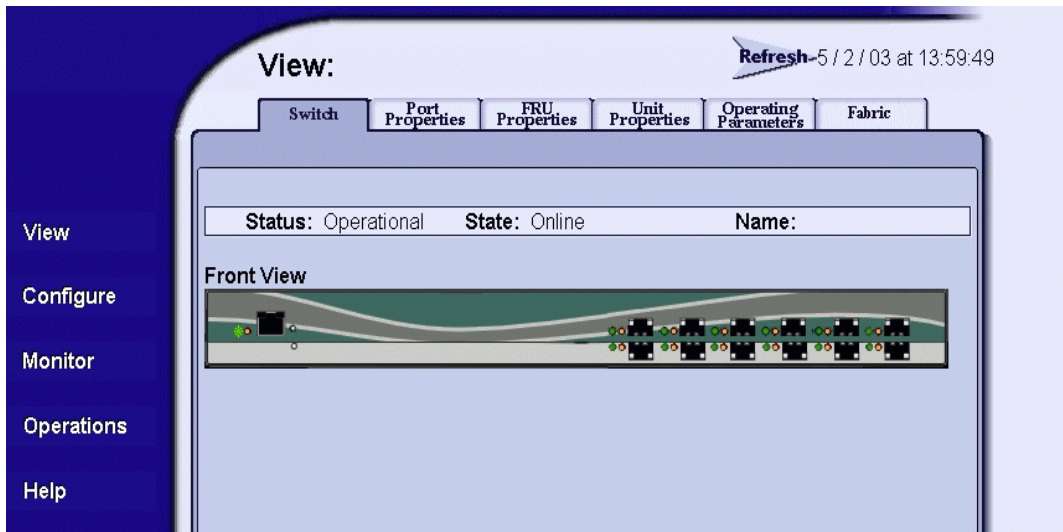


Figure 3-2 View Panel (SANpilot Interface)

Continue to the next step.

5

Does the SANpilot interface appear operational with the *View* panel displayed?

NO YES



Go to [step 10](#).

6

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch control processor (CTP) card failed.

Continue to the next step.

7

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

8

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES

- ↓ A FRU failure or link incident is indicated. **Go to step 18** to obtain event codes that identify the problem. **Exit MAP.**

9

A switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

- a. Wait approximately five minutes, then attempt to login to the switch again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [step 1](#)). The *Username and Password Required* dialog box appears ([Figure 3-1](#) on page 3-7).
- c. Type the user name and password obtained in [step 1](#) and click **OK**. If the *View* panel does not display, wait another five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

YES NO

↓ Perform fault isolation at the switch. **Go to step 20.**

10

At the *View* panel and *Switch* page, inspect the *Status* field at the top of the page.

Does the switch status indicate **Operational**?

NO YES

↓ The switch appears operational. **Exit MAP.**

11

Inspect Fibre Channel port operational states.

- a. At the *View* panel, click the *Port Properties* tab. The *Port Properties* page displays with port **0** highlighted (Figure 3-3).

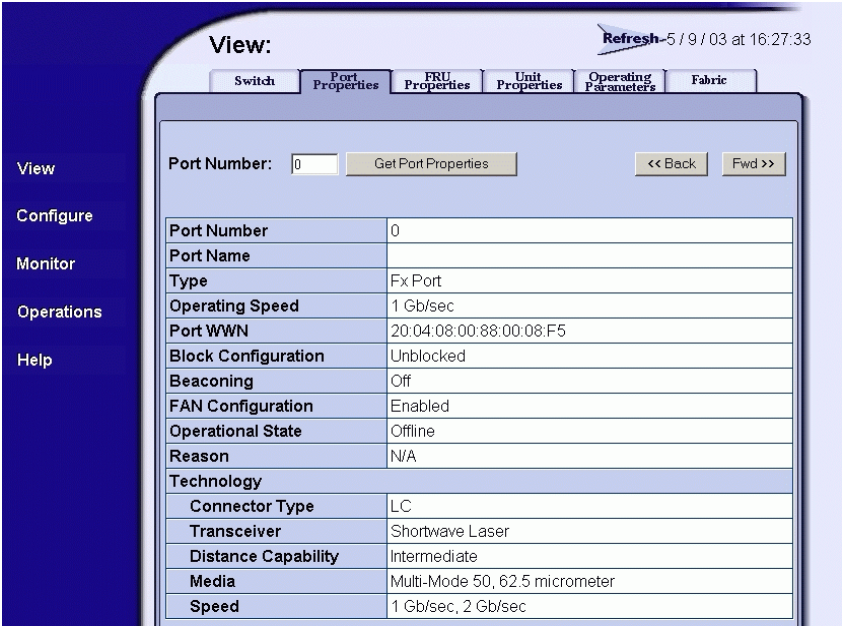


Figure 3-3 View Panel (Port Properties Tab)

- b. Inspect the *Beaconing* and *Operational State* fields.

Does the *Beaconing* field display an **On** message?

YES **NO**

↓ **Go to step 13.**

12

Port beaconing is enabled.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing at the SANpilot interface:
 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Switch* and *Beacon* pages displayed.
 2. Click the *Port* tab. The *Operations* panel opens with the *Port* and *Beacon* pages displayed.
 3. Click the check box (checked) in the *Beaconing State* column and click *Activate* to remove the check mark and disable beaconing. The message **Your changes have been successfully activated** appears.

Continue to the next step.

13

At the *View* panel, does the *Operational State* field display a **Segmented** message?

NO **YES**

↓ Port segmentation is indicated. **Go to step 18** to obtain event codes. If no event codes are found, go to [MAP 0600: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-54. **Exit MAP.**

14

At the *View* panel, does the *Operational State* field display a message indicating a port problem?

NO **YES**

↓ **Go to step 18** to obtain event codes. If no event codes are found, go to [MAP 0500: Port Failure and Link Incident Analysis](#) on page 3-35. **Exit MAP.**

15

Repeat [step 11](#) through [step 14](#) for each remaining Fibre Channel port for which a problem is suspected (ports **0** through **11**).

Is a problem indicated for any of the ports?

NO **YES**



Go to [step 18](#) to obtain event codes. If no event codes are found, go to [MAP 0500: Port Failure and Link Incident Analysis](#) on page 3-35. **Exit MAP.**

16

Inspect the power supply operational state.

- a. At the *View* panel, click the *FRU Properties* tab. The *FRU Properties* page displays ([Figure 3-4](#)).

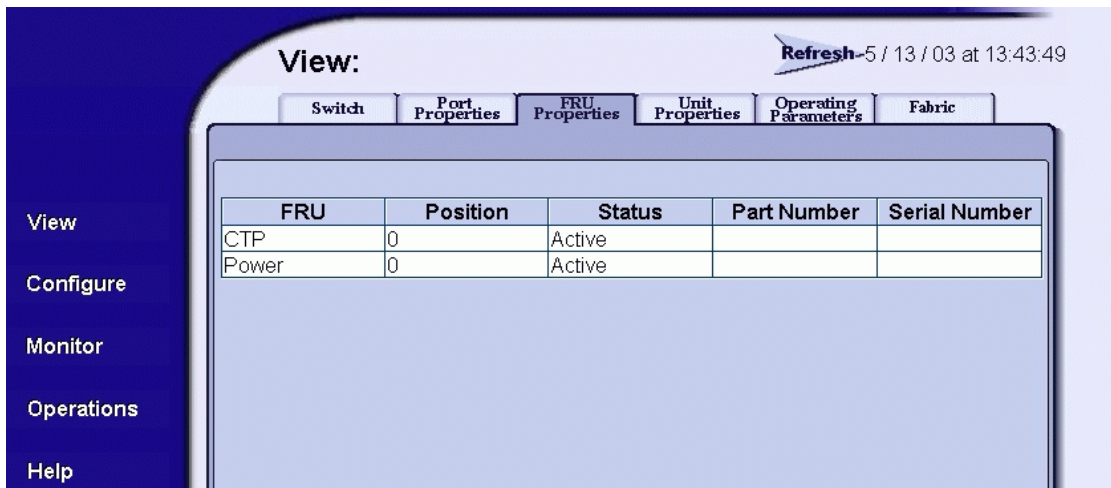


Figure 3-4 View Panel (FRU Properties Tab)

- b. Inspect the *Status* field for the power supply.

Does the *Status* field display a **Failed** message for the power supply?

NO **YES**



A power supply failure is indicated. **Go to [step 18](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

17

Inspect the *Status* fields for switch FRUs.

Does the *State* field display a **Failed** message for any of the FRUs?

YES NO

↓ The switch appears operational. **Exit MAP.**

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to [MAP 0400: FRU Failure Analysis](#) on page 3-30. **Exit MAP.**

18

Obtain event codes from the SANpilot *Event Log*.

NOTE: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

- At the *View* panel, select *Monitor* at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed.
- Click the *Logs* tab. The *Logs* page displays ([Figure 3-5](#)).

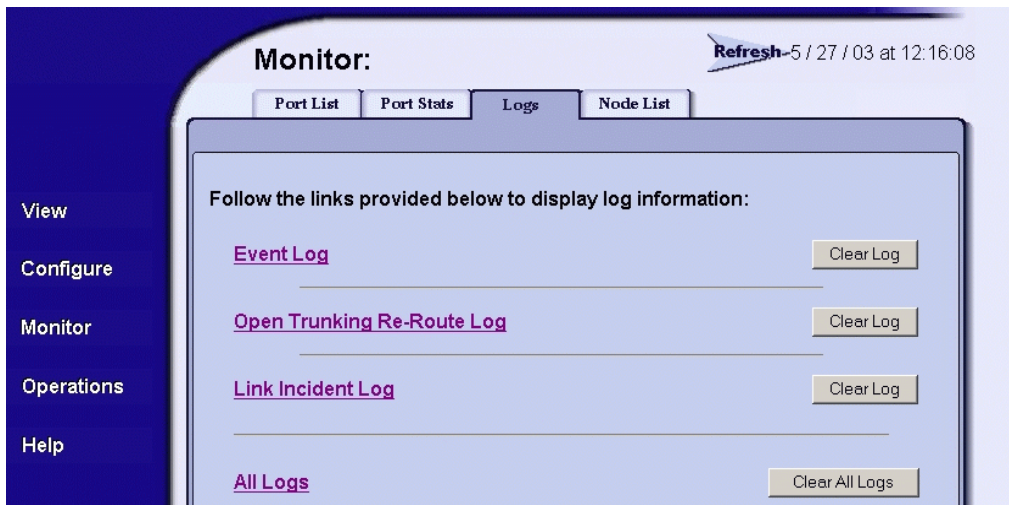


Figure 3-5 Monitor Panel (Logs Page)

- c. Click the *Event Log* entry. The *Event Log* ([Figure 3-6](#)) displays.

Date/Time	Error Code	Severity	Event Data
5/28/03 2:46 pm	410	Informational	44
5/28/03 2:46 pm	453	Informational	0480 0000 0000 0000 0000 0000 0000 0000
5/28/03 2:46 pm	421	Informational	3036 2E30 302E 3030 2031 3900 0000 0000
5/28/03 2:44 pm	423	Informational	
5/28/03 2:43 pm	410	Informational	44
5/28/03 2:43 pm	453	Informational	0480 0000 0000 0000 0000 0000 0000 0000
5/28/03 2:43 pm	421	Informational	3036 2E30 302E 3030 2031 3900 0000 0000
5/28/03 2:40 pm	423	Informational	

Figure 3-6 Event Log

- d. Record the event code, date, time, and severity (*Informational, Minor, Major, or Severe*).
- e. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO YES



Go to [Table 3-3](#) on page 3-3 to interpret event codes. Exit MAP.

Return to [step 1](#) and perform fault isolation again. If this is the second time at this step, contact the next level of support. Exit MAP.

19

Are you at the switch reporting the problem?

YES NO



Go to [step 29](#).

20

Is the green **PWR** LED at the switch front bezel illuminated?

NO YES



Go to [step 25](#).

21

Is the switch connected to facility AC power?

NO **YES**



Go to [step 24](#).

22

Connect the switch to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**



A power distribution problem is indicated. **Go to [step 18](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

23

Is the green **PWR** LED at the switch front bezel illuminated?

NO **YES**



Go to [step 25](#).

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. **Exit MAP.**

24

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



A power distribution problem is indicated. **Go to step 18** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. **Exit MAP.**

25

Is the amber **ERR** LED at the switch front bezel blinking?

YES NO



Go to step 27.

26

Unit beaconing is enabled for the switch.

- a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
- b. Disable unit beaconing at the SANpilot interface.
 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Switch* and *Beacon* pages displayed.
 2. Click *Deactivate* to disable beaconing. The message **Your changes have been successfully activated** appears.

Was unit beaconing enabled because switch failure or degradation was suspected?

YES NO



The switch appears operational. **Exit MAP.**

Go to step 20 and perform fault isolation again (at the switch). If this is the second time at this step, contact the next level of support. **Exit MAP.**

27

Is the amber **ERR** LED at the switch front bezel illuminated?

YES NO



The switch appears operational. **Exit MAP.**

28

Check FRUs for failure symptoms.

Are any amber LEDs associated with Fibre Channel ports illuminated?

NO YES



A Fibre Channel port failure is indicated. **Go to step 18** to obtain event codes. If no event codes are found, go to [MAP 0500: Port Failure and Link Incident Analysis](#) on page 3-35. **Exit MAP.**

A link incident is indicated. **Go to step 18** to obtain event codes. If no event codes are found, go to [MAP 0500: Port Failure and Link Incident Analysis](#) on page 3-35. **Exit MAP.**

29

You are at the console of an open systems interconnection (OSI) server attached to the switch reporting the problem. If an incident occurs on the Fibre Channel link between the switch and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the switch-attached OSI server?

YES NO



Perform fault isolation at the switch. **Go to step 20.**

30

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

581 - Link interface incident - implicit incident.

582 - Link interface incident - bit-error threshold exceeded.

583 - Link failure - loss of signal or loss of synchronization.

584 - Link failure - not-operational primitive sequence received.

585 - Link failure - primitive sequence timeout.

586 - Link failure - invalid primitive sequence received for the current link state.

Were one or more event codes found?

YES NO

↓ Perform fault isolation at the switch. **Go to step 20.**

Go to Table 3-3 on page 3-3 to interpret event codes. Exit MAP.

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including a defective AC power cord or power supply.

1

Is fault isolation being performed at the switch?

YES NO

↓ Fault isolation is being performed at the SANpilot interface.
Go to step 8.

2

Verify the switch is connected to facility power and is powered on.

- a. Ensure the AC power cord is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
- b. Ensure the associated facility circuit breaker is on. If not, ask the customer to set the circuit breaker on.
- c. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES NO

↓ **Go to step 4.**

3

Verify power supply and switch operation. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES NO

↓ The switch appears operational. **Exit MAP.**

4

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for the power supply.
- Input power between 100 and 240 VAC, and at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES NO

↓ Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

5

Verify power supply and switch operation. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES NO

↓ The switch appears operational. **Exit MAP.**

6

The power supply may be operational, but the CTP card is not receiving DC power. The in-card circuit breaker may have tripped due to a power surge, or the CTP card failed. Disconnect the power cord, then reconnect the cord (power cycle the switch) to reset the CTP card.

Did power cycling the switch solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

7

Visual inspection indicates a power supply, power distribution system, or CTP card failure. Replace the switch. **Exit MAP.**

8

Does the SANpilot interface appear operational?

NO **YES**



Go to [step 11](#).

9

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

10

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Is a power supply or power distribution system failure indicated?

YES **NO**



Analysis for an Ethernet link or CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

11

Inspect the power supply operational state at the SANpilot interface.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- b. Inspect the *Status* field for the power supply.

Does the *Status* field display a **Failed** message for the power supply?

NO **YES**

↓ The power supply failed. Replace the switch. **Exit MAP.**

The switch appears operational. **Exit MAP.**

MAP 0200: POST Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial machine load (IML) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IML process.

If an error occurs, the POST/IML process continues in an attempt to initialize the switch and bring it online. An event code **400** displays when the switch completes the POST/IML process.

1

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

2

Was an event code **400** or **411** observed at the SANpilot *Event Log*?

YES NO



Analysis for the failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. Exit MAP.

3

[Table 3-4](#) on page 3-22 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 3-4 MAP 200 Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 4 .
411	Firmware fault.	Go to step 8 .

4

POST/IML diagnostics detected a FRU failure as indicated by event code **400** with supplementary event data.

- At the SANpilot *Event Log*, examine the first two bytes (**0** and **1**) of event data associated with event code **400**.
- Byte **0** is a FRU code that indicates the failed FRU. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU).

[Table 3-5](#) lists byte **0** FRU codes and associated steps that describe fault isolation procedures.

Table 3-5 MAP 200 Byte 0 FRU Codes

Byte 0	Failed FRU	Action
02	CTP card.	Go to step 5 .
05	Fan module.	Go to step 6 .
06	Power supply.	Go to step 7 .

5

The CTP card failed POSTs as indicated by FRU code **02**. Replace the switch. **Exit MAP.**

6

A cooling fan failed POSTs as indicated by FRU code **05**. Replace the switch. **Exit MAP.**

7

The power supply failed POSTs as indicated by FRU code **06**. Replace the switch. **Exit MAP.**

8

POST/IML diagnostics detected a firmware failure as indicated by event code **411** and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily logout, login, and resume operation.

Perform the data collection procedure and return the diskette to McDATA for analysis. **Exit MAP.**

MAP 0300: Loss of Web Browser PC Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and a web browser PC running the SANpilot interface. The failure indication is a **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message.

ATTENTION ! Prior to servicing a product, determine the Ethernet LAN configuration. Installation of products on a public customer intranet can complicate problem determination and fault isolation.

1

Does the SANpilot interface appear operational?

NO YES



The switch-to-SANpilot PC connection is restored and appears operational. The cause may be an Ethernet adapter reset (on the switch CTP card) in response to an error. The connection to the web browser PC terminates briefly, then recovers upon reset.

If this intermittent problem continues, perform the data collection procedure and return the diskette to McDATA for analysis. **Exit MAP.**

2

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

3

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-18. **Exit MAP.**

4

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO YES



A FRU failure or link incident is indicated. Go to [MAP 0000: Start MAP](#) on page 3-6. **Exit MAP.**

5

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

- a. Wait approximately five minutes, then attempt to login to the switch again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the switch (obtained in [MAP 0000: Start MAP](#) on page 3-6). The *Username and Password Required* dialog box appears.
- c. Type the user name and password obtained in [MAP 0000: Start MAP](#) on page 3-6, and click **OK**. If the *View* panel does not display, wait five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

NO **YES**

- ↓ The switch-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

6

A problem with another LAN-attached device may be indicated.

- If the problem is associated with another switch or server, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem for that device. **Exit MAP.**
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO **YES**

- ↓ The switch-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

7

The IP address defining the switch to the Ethernet LAN must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the switch IP address. The tools

are provided with the switch or by service personnel. To verify the IP address:

- a. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a phillips-tip screwdriver may be required). Connect the RS-232 null modem cable to the port.
- b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
- c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
- d. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

NOTE: The following steps describe inspecting the IP address using HyperTerminal serial communication software.

- e. At the *Windows Workstation* menu, sequentially select *Programs*, *Accessories*, *HyperTerminal*, and *HyperTerminal*. The *Connection Description* dialog box displays (Figure 3-7).



Figure 3-7 Connection Description Dialog Box

- f. Type **Sphereon 4300** in the *Name* field and click *OK*. The *Connect To* dialog box displays (Figure 3-8).



Figure 3-8 Connect To Dialog Box

- g. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click *OK*. The *COMn* dialog box displays, where *n* is 1 or 2 ([Figure 3-9](#)).

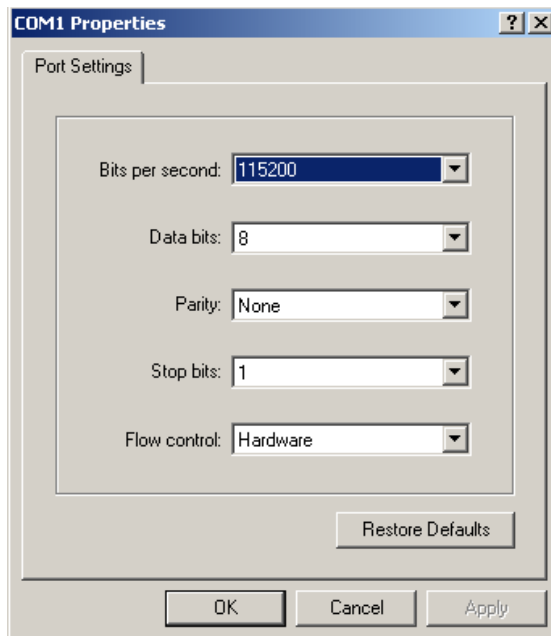


Figure 3-9 COMn Properties Dialog Box

h. Configure the *Port Settings* parameters as follows:

- *Bits per second* - **115200**.
- *Data bits* - **8**.
- *Parity* - **None**.
- *Stop bits* - **1**.
- *Flow control* - **Hardware** or **None**.

When the parameters are set, click **OK**. The *Sphereon 4300 - HyperTerminal* dialog box displays.

- i. At the **>** prompt, type the user-level password (default is **password**) and press **Enter**. The password is case sensitive. The *Sphereon 4300 - HyperTerminal* dialog box displays with a **C>** prompt at the bottom of the window.
- j. At the **C>** prompt, type **ipconfig** and press **Enter**. The *Sphereon 4300 - HyperTerminal* dialog box displays with configuration information listed, including the IP address (Figure 3-10).

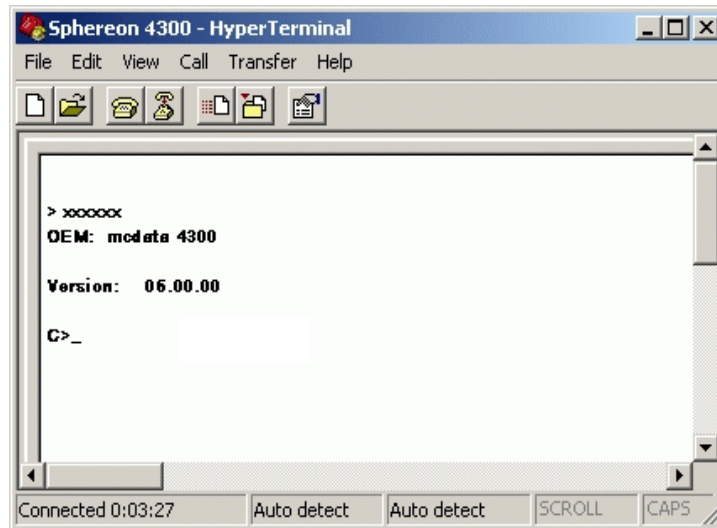


Figure 3-10 Sphereon 4300 - HyperTerminal Dialog Box

- k. Record the switch IP address.
- l. Select *Exit* from the *File* pull-down menu to close the HyperTerminal application. A *HyperTerminal* dialog box displays (Figure 3-11).

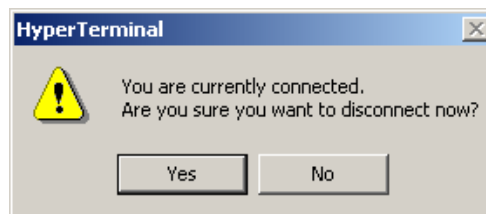


Figure 3-11 HyperTerminal Dialog Box

- m. Click *Yes*. A second *HyperTerminal* dialog box displays (Figure 3-12).

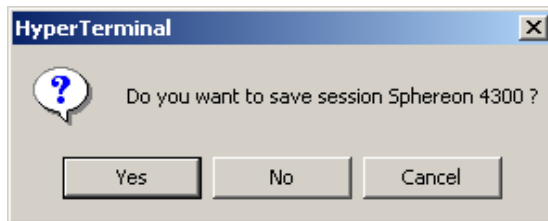


Figure 3-12 HyperTerminal Dialog Box

- n. Click *No* to exit and close the HyperTerminal application.
- o. Power off the maintenance terminal.
- p. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Did changing the IP address of the switch solve the problem?

NO YES

- ↓ The switch-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

Failure of the switch Ethernet port is indicated. Replace the switch.
Exit MAP.

MAP 0400: FRU Failure Analysis

This MAP describes fault isolation for the switch and FRUs. Failure indicators include:

- An event code recorded at the SANpilot *Event Log*.
- The amber LED on the FRU illuminates.
- A **Failed** message associated with a FRU at the SANpilot interface.

1

Was an event code **300, 301, 302, 426, 433, 440, 810, or 811** observed at the SANpilot *Event Log*?

YES NO

- ↓ **Go to [step 3](#).**

2

Table 3-6 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-6 MAP 400 Event Codes

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 6 .
301	Cooling fan propeller failed.	Go to step 6 .
302	Cooling fan propeller failed.	Go to step 6 .
426	Multiple ECC single-bit errors occurred.	Go to step 10 .
433	Non-recoverable Ethernet fault.	Go to step 11 .
440	Embedded port hardware failed.	Go to step 11 .
810	High temperature warning (CTP thermal sensor).	Go to step 10 .
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 10 .

3

Is fault isolation being performed at the switch?

YES NO



Fault isolation is being performed at the SANpilot interface.
Go to [step 12](#).

4

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



An AC power distribution or CTP card failure is indicated. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, replace the switch. **Exit MAP.**

5

Inspect cooling fans at the rear of the switch to ensure all fan blades are rotating.

Does cooling fan inspection indicate a failure (one or more cooling fans not rotating)?

YES NO



Go to step 7.

6

Visual inspection or an event code **300**, **301**, or **302** indicates one or more cooling fans failed. Replace the switch. **Exit MAP.**

7

Inspect the switch front panel.

Is the green **PWR** LED illuminated and the amber **ERR** LED illuminated and blinking (beaconing)?

YES NO



Go to step 9.

8

Unit beaconing is enabled for the switch.

- a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
- b. Disable unit beaconing at the SANpilot interface.
 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Switch* and *Beacon* pages displayed.
 2. Click *Deactivate* to disable beaconing. The message **Your changes have been successfully activated** appears.

Was unit beaconing enabled because a failure or degradation was suspected?

NO YES

↓ **Go to [step 1](#).**

The switch appears operational. **Exit MAP.**

9

Is the green **PWR** LED illuminated, the amber **ERR** LED illuminated, and all Fibre Channel traffic disrupted (not operational)?

NO YES

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Analysis for this failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

10

An event code **426** (SDRAM problem), **810** (high-temperature warning), or **811** (critically-hot temperature warning) indicates an intermittent problem that may result in switch failure.

Is the appearance of this event code a recurring problem?

NO YES

↓ A CTP card failure is indicated. Replace the switch.
Exit MAP.

Perform the data collection procedure and contact the next level of support. Refer to [Collect Maintenance Data](#) on page 4-22. **Exit MAP.**

11

An event code **433** or **440** indicates a CTP card failure. Replace the switch. **Exit MAP.**

12

Does the SANpilot interface appear operational?

NO YES

↓ **Go to [step 14](#).**

13

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

The SANpilot interface is not operational and fault isolation must be performed at the switch. **Go to [step 4](#).**

14

Inspect the power supply (includes fan modules) operational state at the SANpilot interface.

- At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- Inspect the *Status* field for the power supply.

Does the *Status* field display a **Failed** message for the power supply?

NO YES

- ↓ A fan module or power supply failure is indicated. Replace the switch. **Exit MAP.**

15

Inspect the CTP card operational state at the SANpilot interface.

- At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- Inspect the *Status* field for the CTP card.

Does the *Status* field display a **Failed** message for the CTP card?

NO YES

- ↓ A CTP card failure is indicated. Replace the switch. **Exit MAP.**

Additional analysis is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-6. If this is the second time at this step, contact the next level of support. **Exit MAP.**

MAP 0500: Port Failure and Link Incident Analysis

This MAP describes fault isolation for shortwave laser small form factor pluggable (SFP) optical transceivers, longwave laser SFP optical transceivers, and Fibre Channel link incidents. Failure indicators include:

- An event code recorded at the SANpilot *Event Log*.
- A link incident event code recorded at the console of an OSI server attached to the switch reporting the problem.
- One or more amber LEDs on the ports illuminate.
- A port operational state message or a **Failed** message associated with a port at the SANpilot interface.

1

Was an event code **080**, **081**, **506**, **507**, **512**, or **514** observed at the SANpilot *Event Log*?

NO YES
↓ Go to [step 3](#).

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the switch reporting the problem?

YES NO
↓ Go to [step 4](#).

3

[Table 3-7](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-7 MAP 500 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 13 .
081	Invalid attachment.	Go to step 24 .
506	Fibre Channel port failure.	Go to step 6 .

Table 3-7 MAP 500 Event Codes

Event Code	Explanation	Action
507	Loopback diagnostics port failure.	Go to step 14 .
512	SFP optical transceiver nonfatal error.	Go to step 6 .
514	SFP optical transceiver failure.	Go to step 6 .
581	Implicit incident.	Go to step 17 .
582	Bit error threshold exceeded.	Go to step 17 .
583	Loss of signal or loss of synchronization.	Go to step 17 .
584	Not operational primitive sequence received.	Go to step 17 .
585	Primitive sequence timeout.	Go to step 17 .
586	Invalid primitive sequence received for current link state.	Go to step 17 .

4

Is fault isolation being performed at the switch?

YES NO



Fault isolation is being performed at the SANpilot interface.
Go to [step 7](#).

5

Each port has an amber LED and a blue (2 Gbps operation) or green (1 Gbps operation) LED adjacent to the port. The amber LED illuminates and the blue or green LED extinguishes if the port fails.

Is an amber port LED illuminated but not blinking (beaconing)?

YES NO



The switch appears operational, however a link incident or other problem may have occurred. **Go to [step 16](#).**

6

As indicated by a visual inspection, message, or event code **506**, **512**, or **514**, a Fibre Channel port failed and the SFP optical transceiver must be removed and replaced. Refer to [RRP 1: SFP Optical Transceiver](#) on page 5-2.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-19.

NOTE: An event code 514 may generate a call-home event that incorrectly indicates a CTP card failure. Although the optical socket may have failed, first replace the optical transceiver and verify operation. If a failure is still indicated, replace the switch. When an even code 514 is indicated, ensure a replacement optical transceiver and a replacement switch are available.

Did SFP optical transceiver replacement solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

Does the SANpilot interface appear operational?

NO YES

↓ **Go to [step 10](#).**

8

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

9

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES NO



Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

10

Inspect Fibre Channel port operational states at the SANpilot interface.

- a. At the *View* panel, click the *Port Properties* tab. The *Port Properties* page displays with port **0** properties displayed.
- b. Click the port number (**0** through **11**) for which a failure is suspected to display properties for that port.
- c. Inspect the *Operational State* field. Scroll down the *View* panel as necessary.
- d. [Table 3-8](#) lists port operational states and MAP steps that describe fault isolation procedures.

Table 3-8 Port Operational States and Actions

Operational State	Action
Online	No action required. Exit MAP.
Port Failure	Go to step 6 .
Offline	Go to step 11 .
Not Operational	Go to step 11 .
Testing	Internal or external loopback test in process. Exit MAP.

Table 3-8 Port Operational States and Actions (Continued)

Operational State	Action
Not Installed	Go to step 12 .
Invalid Attachment	Go to step 24 .
Link Reset	Go to step 35 .
Inactive	Go to step 36 .
No light	Go to step 40 .
Segmented E_Port	Go to MAP 0600 .

11

A switch port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline, and to take the appropriate corrective action. **Exit MAP.**

12

Install an SFP optical transceiver in the port receptacle. Refer to [RRP 1: SFP Optical Transceiver](#) on page 5-2.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the uninstalled port.
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-19.

Exit MAP.

13

As indicated by a message or event code **080**, the eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device. Inspect port binding parameters at the SANpilot interface

- a. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.

- b. Click the *Security* tab, then click the *Port Binding* tab. The *Port Binding* page displays.
- c. Inspect entries the *Port WWN* column. These are WWNs assigned to the port or Fibre Channel interface installed on the attached device.
 - If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
 - If a nickname is assigned to the WWN, the nickname appears in place of the WWN.
- d. The bound WWN must be entered in the form of a raw WWN format (**XX:XX:XX:XX:XX:XX:XX:XX**) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

14

As indicated by event code **507**, a Fibre Channel port failed an internal or external loopback test.

- a. At the SANpilot interface, reset each port that failed the loopback test.
 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Switch* and *Beacon* pages displayed.
 2. Click the *Port* tab. The *Operations* panel opens with the *Port* and *Beacon* pages displayed.
 3. Click the *Reset* tab. The *Reset* page displays.
 4. Click the check box (checked) in the *Port Reset* column and click *Activate* to reset the port. The message **Your changes have been successfully activated** appears.
- b. Perform an external loopback test for all ports that were reset. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-19.

Did resetting ports solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

15

Port beaconing may be enabled.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing at the SANpilot interface:
 1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Switch* and *Beacon* pages displayed.
 2. Click the *Port* tab. The *Operations* panel opens with the *Port* and *Beacon* pages displayed.
 3. Click the check box (checked) in the *Beaconing State* column and click *Activate* to remove the check mark and disable beaconing. The message **Your changes have been successfully activated** appears.

Was port beaconing enabled because port failure or degradation was suspected?

YES NO



The switch appears operational. **Exit MAP.**

Go to [step 1](#).

16

A link incident may have occurred. Inspect the *Link Incident Log* at the SANpilot interface

- a. At the *View* panel, select *Monitor* at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed.
- b. Click the *Logs* tab, then click the *Link Incident Log* entry. The *Link Incident Log* displays ([Figure 3-13](#)).

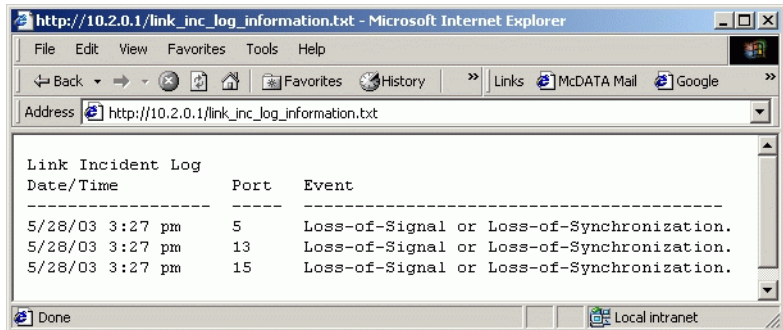


Figure 3-13 Link Incident Log

- c. If a link incident occurred, the affected port number is listed with one of the following messages.

Link interface incident - implicit incident.

Link interface incident - bit-error threshold exceeded.

Link failure - loss of signal or loss of synchronization.

Link failure - not-operational primitive sequence (NOS) received.

Link failure - primitive sequence timeout.

Link failure - invalid primitive sequence received for the current link state.

Did one of the listed messages appear in the *Link Incident Log*?

YES NO

↓ The switch appears operational. **Exit MAP.**

17

A link incident message appeared in the *Link Incident Log* or an event code **581, 582, 583, 584, 585, or 586** was observed at the console of an OSI server attached to the switch reporting the problem.

Clear the *Link Incident Log* at the SANpilot interface:

- a. At the *View* panel, select *Monitor* at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed.
- b. Click the *Logs* tab, then click the *Clear Log* button adjacent to the *Link Incident Log* entry. An **Are you sure you want to clear the Link Incident Log?** message box displays.

- c. Click *OK*. The message **Your changes have been successfully activated** appears.

After clearing the log, did the link incident recur?

YES NO

- ↓ The problem is transient and the Fibre Channel link and switch appear operational. **Exit MAP.**

18

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

- Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- Block the port. Refer to [Block or Unblock a Port](#) on page 4-26.
- Remove and replace the fiber-optic jumper cable.
- Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-26.

Was a corrective action performed?

YES NO

- ↓ **Go to [step 20](#).**

19

Monitor port operation for approximately five minutes.

Did a link incident or *No Light* message recur?

YES NO

- ↓ The Fibre Channel link and switch appear operational.
Exit MAP.

20

Clean fiber-optic connectors on the jumper cable.

- Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- Block the port. Refer to [Block or Unblock a Port](#) on page 4-26.
- Disconnect both ends of the fiber-optic cable.

- d. Clean the fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-28.
- e. Reconnect the fiber-optic cable.
- f. Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-26.
- g. Monitor port operation for approximately five minutes.

Did a link incident or *No Light* message recur?

YES NO

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

21

Disconnect the fiber-optic jumper cable from the switch port and connect the cable to a spare port.

Is link incident or *No Light* message occur at the new port?

YES NO

↓ **Go to [step 23](#).**

22

The attached device is causing the recurrent link incident or *No Light* message. Notify the customer of the problem and have the system administrator:

- a. Inspect and verify operation of the attached device.
- b. Repair the attached device if a failure is indicated.
- c. Monitor port operation for approximately five minutes.

Did a link incident or *No Light* message recur?

YES NO

↓ The attached device, Fibre Channel link, and switch appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

23

The switch port reporting the problem is causing the recurrent link incident or *No Light* message. The recurring problem indicates port degradation and a possible pending failure. **Go to [step 6](#).**

24

As indicated by a message or event code **081**, a port has an invalid attachment. The information in the *Port Properties* dialog box specifies the reason as listed in [Table 3-9](#).

Table 3-9 Invalid Attachment Reasons and Actions

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed.	Go to step 25 .
Incompatible switch.	Go to step 26 .
External loopback plug connected.	Go to step 27 .
N-Port connection not allowed.	Go to step 25 .
Non-McDATA switch at other end.	Go to step 26 .
Unauthorized port binding WWN.	Go to step 13 .
Unresponsive node.	Go to step 29 .
ESA security mismatch.	Go to step 31 .
Fabric binding mismatch.	Go to step 32 .
Authorization failure reject.	Go to step 29 .
Unauthorized switch binding WWN.	Go to step 33 .
Fabric mode mismatch.	Go to step 26 .
CNT WAN extension mode mismatch.	Go to step 34 .

25

The port connection conflicts with the configured port type and an ISL connection is not allowed. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element.

- At the SANpilot interface *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- At the *Type* column, click the arrow adjacent to the list box for the port and select a port type as follows:

- Select fabric port (**F_Port**) if the port is cabled to a device (node).
 - Select expansion port (**E_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.
- c. Click *Activate* to save the change. The message **Your changes to the port configuration have been successfully activated** appears.

Did reconfiguring the port type solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

26



One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy McDATA switch at the incorrect Exchange Link Parameter (ELP) revision level.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a non-McDATA switch at the incorrect ELP revision level.
- The switch is configured for operation in **McDATA Fabric 1.0** mode and is connected to a non-McDATA switch.

Reconfigure the switch operating mode:

- Ensure the switch is set offline. Refer to [Set the Switch Online or Offline](#) on page 4-25.
- At the SANpilot interface *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- Click the *Switch* tab, then click the *Fabric Parameters* tab. The *Fabric Parameters* page displays.
- Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* list box.

- Select the **McDATA Fabric 1.0** option if the switch is fabric-attached *only* to other McDATA directors or switches that are also operating in **McDATA Fabric 1.0** mode.
- Select the **Open Fabric 1.0** option if the switch is fabric-attached to directors or switches produced by other original equipment manufacturers (OEMs) that are open-fabric compliant.

e. Click *Activate* to save the change. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.

Did configuring the operating mode solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

27

A loopback (wrap) plug appears to be connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES NO

↓ Contact the next level of support. **Exit MAP.**

28

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational and a device is attached, the blue or green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Did removing the loopback plug solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

29

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

- a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port. Refer to [Block or Unblock a Port](#) on page 4-26.
- c. Disconnect both ends of the fiber-optic cable.
- d. Clean the fiber-optic connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-28.
- e. Reconnect the fiber-optic cable.
- f. Unblock the port. Refer to [Block or Unblock a Port](#) on page 4-26.
- g. Monitor port operation for approximately five minutes.

Is the invalid attachment problem solved?

YES NO

- ↓ The Fibre Channel link and switch appear operational.
Exit MAP.

30

Inspect and service the host bus adapters (HBAs) as necessary.

Did service of the HBAs solve the problem?

NO YES

- ↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

31

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch between two fabric elements. The SANtegrity binding feature must be enabled on both switches, and switch and fabric binding parameters must be compatible. At the SANpilot interface for both switches:

- a. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.

- b. Click the *Security* tab, then click the *Switch Binding* tab. The *Switch Binding* page displays.
- c. Ensure the switch binding state is enabled (noted at the top of the page) for both switches.
- d. Ensure the *Connection Policy* (**Enable & Restrict E_Ports, Enable & Restrict F_Ports, Enable & Restrict All Ports, or Disable Switch Binding**) is compatible for both switches.
- e. The *Attached Nodes* drop-down list contains the world wide names of attached Fibre Channel devices. Ensure these switch binding membership lists are compatible for both switches
 - To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, select a WWN from the *Attached Nodes* drop-down list and click the adjacent *Add Member* button; or type a new WWN in the *Detached Node (WWN)* field and click the adjacent *Add Member* button.
 - To delete a device from the switch binding membership list, click the *Delete* button adjacent to the device WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the device.
- f. Click *Submit*. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.
- g. Click the *Fabric Binding* tab. The *Fabric Binding* page displays.
- h. Ensure the fabric binding membership lists are compatible for both switches
 - To add a member (new fabric) to the fabric binding membership list displayed at the bottom of the page, type a new domain ID (range is **1** through **31**) in the *Domain ID* field, type a new WWN in the *WWN* field, and click the adjacent *Add Member* button.
 - To delete a fabric from the fabric binding membership list, click the *Delete* button adjacent to the fabric domain ID and WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the fabric.
- i. Click *Save and Activate* to save and activate the displayed fabric binding configuration. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the fabric binding configuration, and change the status to **Saved & Active**.

Did configuring the fabric and switch binding parameters solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

32

A port connection is not allowed because of a fabric binding mismatch between fabric elements. Fabric binding membership lists must be compatible for both switches. At the SANpilot interface for both switches:

- a. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- b. Click the *Security* tab, then click the *Fabric Binding* tab. The *Fabric Binding* page displays.
- c. Ensure the fabric binding membership lists are compatible for both switches
 - To add a member (new fabric) to the fabric binding membership list displayed at the bottom of the page, type a new domain ID (range is **1** through **31**) in the *Domain ID* field, type a new WWN in the *WWN* field, and click the adjacent *Add Member* button.
 - To delete a fabric from the fabric binding membership list, click the *Delete* button adjacent to the fabric domain ID and WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the fabric.
- d. Click *Save and Activate* to save and activate the displayed fabric binding configuration. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the fabric binding configuration, and change the status to **Saved & Active**.

Did updating the fabric binding membership lists solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

33

A port connection is not allowed because of a switch binding mismatch between fabric elements. Switch membership lists must be

compatible for both switches. At the SANpilot interface for both switches:

- a. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- b. Click the *Security* tab, then click the *Switch Binding* tab. The *Switch Binding* page displays.
- c. The *Attached Nodes* drop-down list contains the world wide names of attached Fibre Channel devices. Ensure these switch binding membership lists are compatible for both switches
 - To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, select a WWN from the *Attached Nodes* drop-down list and click the adjacent *Add Member* button; or type a new WWN in the *Detached Node (WWN)* field and click the adjacent *Add Member* button.
 - To delete a device from the switch binding membership list, click the *Delete* button adjacent to the device WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the device.
- d. Click *Submit*. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

Did updating the switch binding membership lists solve the problem?

NO YES

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

34

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to CNT WAN extension mode.

Contact McDATA support personnel to obtain software maintenance release 4.02.00 or higher. This release is required to correct the problem and allow McDATA switches to communicate with CNT UltraEdge WAN Gateways. **Exit MAP.**

35

The switch and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO **YES**

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

Go to [step 1](#).

36

A switch port state is inactive because the Flexport Technology product feature enablement (PFE) key is not installed for the port (Fibre Channel ports **4** through **11** only) or because of a transmission speed conflict between the port configuration and the SFP optical transceiver.

Is the inactive port a:

- Base configuration port (Fibre Channel ports **0** through **3**), or an
- Installed Flexport Technology port (Fibre Channel ports **4** through **11**)?

NO **YES**

↓ **Go to [step 39](#).**

37

Does the customer desire installation of the Flexport Technology PFE key (ports **4** through **7** and/or ports **8** through **11**)?

YES **NO**

↓ The switch appears operational and the *Inactive port* state is acceptable to the customer. No action is required. **Exit MAP.**

38

Install the Flexport Technology PFE key. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38.

Did installation of the key solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

39

A transmission speed conflict between the port configuration and the SFP optical transceiver is indicated.

- a. At the SANpilot interface *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- b. At the *Speed* column, click the arrow adjacent to the list box for the port and select a port speed as follows:
 - Select **1 Gb/sec** if a one gigabit per second (Gbps) optical transceiver is installed in the port.
 - Select **2 Gb/sec** if a two Gbps optical transceiver is installed in the port.
- c. Click *Activate* to save the change. The message **Your changes to the port configuration have been successfully activated** appears.

Did reconfiguring the port speed solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

40

A switch port state indicates *No Light* because a Fibre Channel device is not attached to the port, or a problem exists with the fiber-optic cable, attached device, or SFP optical transceiver.

Is a Fibre Channel device connected to the port?

NO **YES**

↓ **Go to [step 43](#).**

41

Does the customer desire a device connection?

YES **NO**

↓ The switch appears operational and the *No Light* state is acceptable to the customer. No action is required. **Exit MAP.**

42

Connect a Fibre Channel device to the port as directed by the customer.

Did connection of a device to the port solve the problem?

NO **YES**



The switch appears operational. **Exit MAP.**

43

A problem exists with the fiber-optic cable, attached device, or SFP optical transceiver. **Go to [step 18](#).**

MAP 0600: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes fault isolation of fabric logout, interswitch link (ISL), and E_Port segmentation problems. Failure indicators include:

- An event code recorded at the SANpilot *Event Log*.
- A segmentation reason associated with a Fibre Channel port at the SANpilot interface.

1

Base product Fibre Channel ports on the Sphereon 4300 Switch can only be configured as F_Ports or fabric loop (FL_Ports). Installation of the full-fabric PFE key is required to configure ports as E_Ports and enable ISL connections to other fabric elements.

Is the full-fabric PFE key installed on the switch?

NO **YES**



Go to [step 3](#).

2

Does the customer desire installation of the full-fabric PFE key?

YES **NO**



The switch appears operational and the inability to configure E_Ports and connect the switch to another fabric element is acceptable to the customer. No action is required. **Exit MAP.**

Install the full-fabric PFE key. Refer to [Install PFE Keys \(Optional\)](#) on page 2-38. **Exit MAP.**

3

Was an event code **011**, **021**, **051**, **052**, **061**, **062**, **063**, **070**, **071**, **072**, **140**, **142**, or **150** observed at the SANpilot *Event Log*?

YES NO



Go to [step 5](#).

4

[Table 3-10](#) on page 3-55 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 3-10 MAP 600 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to step 7 .
021	Name Server database invalid.	Go to step 7 .
051	Management Server database invalid.	Go to step 8 .
052	Management Server internal error.	Go to step 8 .
061	Fabric Controller database invalid.	Go to step 9 .
062	Maximum interswitch hop count exceeded.	Go to step 10 .
063	Remote switch has too many ISLs.	Go to step 11 .
070	E_Port is segmented.	Go to step 12 .
071	Switch is isolated.	Go to step 12 .
072	E_Port connected to unsupported switch.	Go to step 20 .
140	Congestion detected on an ISL.	Go to step 21 .
142	Low BB_Credit detected on an ISL.	Go to step 22 .
150	Zone merge failure.	Go to step 23 .

5

Go to the web server PC accessing the switch's SANpilot interface.

Does the SANpilot interface appear operational?

YES NO



Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-6](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

6

Inspect the Fibre Channel port segmentation reason at the SANpilot interface.

- At the *View* panel, click the *Port Properties* tab. The *View* panel opens with the *Port Properties* page displayed.
- Click the port number (**0** through **11**) of the segmented port.
- Inspect the *Reason* field for the selected port.

Is the *Reason* field blank or does it display an **N/A** message?

NO YES



The switch ISL appears operational. **Exit MAP.**

The *Reason* field displays a segmentation reason message.

[Table 3-11](#) lists the reasons and associated steps that describe fault isolation procedures.

Table 3-11 Port Segmentation Reasons and Actions

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 13 .
Duplicate domain ID.	Go to step 14 .
Incompatible zoning configurations.	Go to step 15 .
Build fabric protocol error.	Go to step 16 .
No principal switch.	Go to step 18 .
No response from attached switch (hello timeout).	Go to step 19 .

7

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the error:

- **Event code 011** - The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021** - The Name Server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the diskette to McDATA for analysis. **Exit MAP.**

8

A minor error occurred that caused the Management Server database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the error:

- **Event code 051** - The Management Server database failed CRC validation.
- **Event code 052** - An internal operating error was detected by the Management Server subsystem.

All attached devices resume operation after Management Server login. Perform the data collection procedure and return the diskette to McDATA for analysis. **Exit MAP.**

9

As indicated by an event code **061**, a minor error occurred that caused the Fabric Controller database to fail CRC validation and be re-initialized to an empty state. As a result, the switch briefly lost interswitch link capability.

All interswitch links resume operation after CTP reset. Perform the data collection procedure and return the diskette to McDATA for analysis. **Exit MAP.**

10

As indicated by an event code **062**, the Fabric Controller software detected a path to another fabric element (director or switch) in a multiswitch fabric that traverses more than three interswitch links

(hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

NO YES

↓ The switch and multiswitch fabric appear operational.
Exit MAP.

Contact the next level of support. **Exit MAP.**

11

As indicated by an event code **063**, the Fabric Controller software detected an:

- Intrepid 6064 Director in a multiswitch fabric that has more than the proscribed number of ISLs.
- Intrepid 6140 Director in a multiswitch fabric that has more than the proscribed number of ISLs.
- Other fabric element (director or switch) in a multiswitch fabric that has more than the proscribed number of ISLs.

Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems. Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no director or switch elements have more than the proscribed number of ISLs.

Did fabric reconfiguration solve the problem?

NO YES

↓ The switch and multiswitch fabric appear operational.
Exit MAP.

Contact the next level of support. **Exit MAP.**

12

A **070** event code indicates an E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multiswitch fabric. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

- a. At the SANpilot *Event Log*, examine the first five bytes (**0** through **4**) of event data.
- b. Byte **0** specifies the switch port number (**00** through **11**) of the segmented E_port. Byte **4** specifies the segmentation reason as specified in [Table 3-12](#) on page 3-59.

Table 3-12 Byte 4 Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 13 .
02	Duplicate domain ID.	Go to step 14 .
03	Incompatible zoning configurations.	Go to step 15 .
04	Build fabric protocol error.	Go to step 16 .
05	No principal switch.	Go to step 18 .
06	No response from attached switch (hello timeout).	Go to step 19 .

13

A switch E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

- a. Contact McDATA customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both switches.
- b. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
- c. Set both switches offline. Refer to [Set the Switch Online or Offline](#) on page 4-25.
- d. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.

- e. Click the *Switch* tab, then click the *Fabric Parameters* tab. The *Fabric Parameters* page displays.
- f. Type the recommended E_D_TOV and R_A_TOV values, then click *Activate* to save the change. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.
- g. Repeat steps **d** through **f** for the switch attached to the segmented E_Port (second switch). Use the same E_D_TOV and R_A_TOV values.
- h. Set both switches online. Refer to [Set the Switch Online or Offline](#) on page 4-25.

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

- ↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

14

A switch E_Port segmented because two fabric elements had duplicate domain IDs.

- a. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each switch.
- b. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
- c. Set both switches offline. Refer to [Set the Switch Online or Offline](#) on page 4-25.
- d. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- e. Click the *Switch* tab, then click the *Parameters* tab. The *Parameters* page displays.
- f. Type the customer-determined preferred domain ID value, then click *Activate* to save the change. The message **Your changes to the operating parameters configuration have been successfully activated** appears.

- g. Repeat steps **d** through **f** for the switch attached to the segmented E_Port (second switch). Use a different preferred domain ID value.
- h. Set both switches online. Refer to [Set the Switch Online or Offline](#) on page 4-25.

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

- ↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

15

A switch E_Port segmented because two switches had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

- a. Work with the system administrator to determine the desired zone name change for one of the affected switches. Zone names must conform to the following rules:
 - The name must be 64 characters or fewer in length.
 - The first character must be a letter (**a** through **z**), upper or lower case.
 - Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**\$**), hyphen (**-**), caret (**^**), or underscore (**_**).
- b. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- c. Click the *Zoning* tab, then click the *Zones* tab. The *Zones* page displays.
- d. Inspect zone names (listed under *Display Previous Zones*) in the active zone set to determine the incompatible name.
- e. Modify the incompatible zone name as directed by the customer. Refer to [Task 6: Configure Zoning \(Optional\)](#) on page 2-46.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A switch E_Port segmented because a build fabric protocol error was detected.

- a. Disconnect the fiber-optic jumper cable from the segmented E_Port.
- b. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

17

Initial machine load (IML) the switch. Refer to [IML or Reset the Switch](#) on page 4-30.

Did the IML solve the problem and did both switches join through the ISL to form a fabric?

NO YES

↓ The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Perform the data collection procedure and contact the next level of support. **Exit MAP.**

18

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

- a. Notify the customer the switch will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

- b. Set the switch offline. Refer to [Set the Switch Online or Offline](#) on page 4-25.
- c. At the *View* panel, select *Configure* at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
- d. Click the *Switch* tab, then click the *Fabric Parameters* tab. The *Fabric Parameters* page displays. The switch priority value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric switches (including itself).

Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means that the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a multiswitch fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment and the message *No Principal Switch* appears in the *Reason* field of the *Port Properties* page.

- e. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default* (the default setting is *Default*), then click *Activate* to save the change. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.
- f. Set the switch online. Refer to [Set the Switch Online or Offline](#) on page 4-25.

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO YES



The switch, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

19

A switch *E_Port* segmented (at an operational switch) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

- a. Perform the data collection procedure at the operational switch and return the diskette to McDATA for analysis. This information may assist in fault isolating the failed switch.
- b. Go to [MAP 0000: Start MAP](#) on page 3-6 and perform fault isolation for the failed switch.

Exit MAP.

20

As indicated by an event code **072**, a switch E_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. **Exit MAP.**

21

A **140** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

NO YES

↓ The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

22

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gbps to 2 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB_Credit condition?

NO YES

↓ The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

23

A **150** event code indicates a zone merge process failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

- a. At the SANpilot *Event Log*, examine the first 12 bytes (**0** through **11**) of event data.
- b. Bytes **0** through **3** specify the E_Port number (**00** through **11**) reporting the problem. Bytes **8** through **11** specify the failure reason as specified in [Table 3-13](#).

Table 3-13 Bytes 8 through 11 Failure Reasons and Actions

Bytes 8 - 11	Failure Reason	Action
01	Invalid data length.	Go to step 24 .
08	Invalid zone set format.	Go to step 24 .
09	Invalid data.	Go to step 25 .
0A	Cannot merge.	Go to step 25 .
F0	Retry limit reached.	Go to step 24 .
F1	Invalid response length.	Go to step 24 .
F2	Invalid response code.	Go to step 24 .

24

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 01** - An invalid data length condition caused an error in a zone merge frame.
- **Failure reason 08** - An invalid zone set format caused an error in a zone merge frame.
- **Failure reason F0** - A retry limit reached condition caused an error in a zone merge frame.
- **Failure reason F1** - An invalid response length condition caused an error in a zone merge frame.
- **Failure reason F2** - An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and was the resulting zone merge process successful?

NO YES

↓ The merged zone appears operational. **Exit MAP.**

Perform the data collection procedure and return the diskette to McDATA for analysis. Contact the next level of support. **Exit MAP.**

25

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 09** - Invalid data caused a zone merge failure.
- **Failure reason 0A** - A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code. At the SANpilot *Event Log*, examine bytes **12** through **15** of event data that specify the error code. Record the error code and supplementary error code data.

Perform the data collection procedure and return the diskette to McDATA for analysis. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. **Exit MAP.**

This chapter describes repair-related procedures for the Sphereon 4300 Switch and associated field-replaceable units (FRUs). The procedures are performed through the SANpilot interface. The following procedures are described:

- Obtain log information.
- Obtain port diagnostic information.
- Perform port diagnostic loopback tests.
- Collect maintenance data.
- Set the switch online or offline.
- Block or unblock Fibre Channel ports.
- Clean fiber-optic components.
- Power the switch on and off.
- Perform a switch reset or initial machine load (IML).
- Manage firmware versions.
- Manage configuration data.
- Install or upgrade software.

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to [MAP 0000: Start MAP](#) on page 3-6.

Procedural Notes

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all **WARNING** statements, and statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

Obtain Log Information

The SANpilot interface provides access to the following logs that contain information for maintenance personnel:

- Event Log.
- Open Trunking Re-Route Log.
- Link Incident Log.
- Security Log
- Audit Log
- Fabric Log
- Embedded Port Frame Log

To open a log, click the *Logs* tab at the *Monitor* panel. The *Monitor* panel opens with the *Logs* page displayed ([Figure 4-1](#) on page 4-3). At the *Logs* page:

- Select (double-click) a log title to open and view the contents of the associated log, or
- Select (double-click) the *All Logs* title to open and simultaneously view the contents of all logs.

The *Logs* page provides a *Clear Log* button for each log. Click the button to delete all entries for the associated log. The *Logs* page also

provides a *Clear All Logs* button. Click the button to delete all entries in all logs.

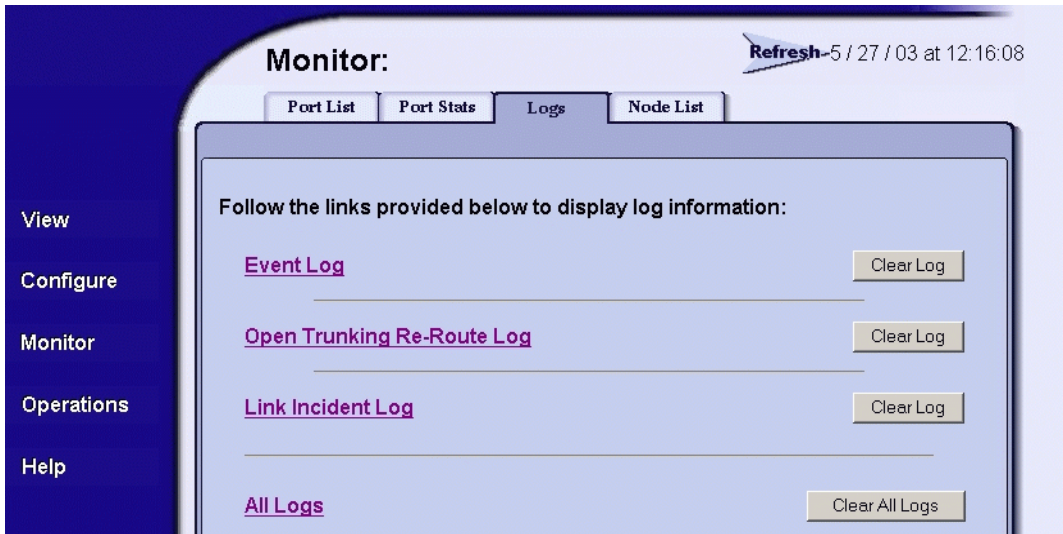


Figure 4-1 Monitor Panel (Logs Page)

Event Log

The *Event Log* (Figure 4-2) displays events or errors recorded at the SANpilot interface. Entries reflect the status of the interface and managed switch. The log stores up to 200 entries, and the most recent entry appears at the top of the log.

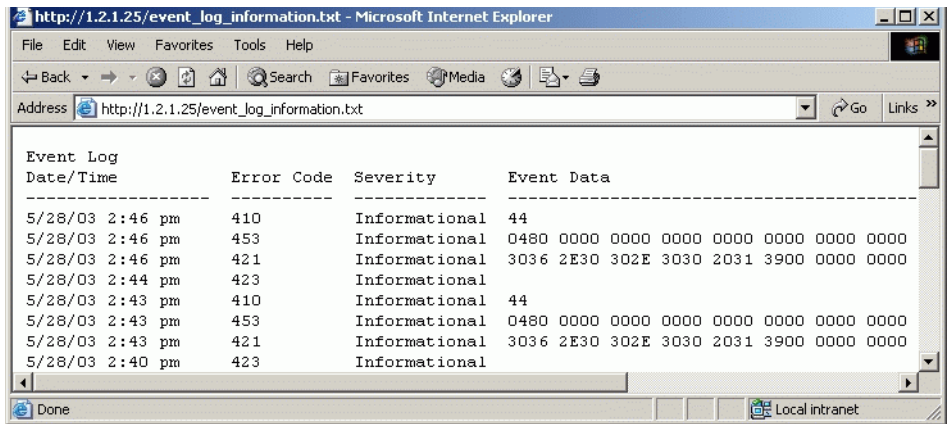


Figure 4-2 Event Log

Open Trunking Re-Route Log

The log consists of the following columns:

- **Date/Time** - Date and time the event occurred.
- **Error Code** - Three-digit code that describes the event. Event codes are listed and described in [Appendix A, Event Code Tables](#).
- **Severity** - Severity of the event (*Informational, Minor, Major, or Severe*).
- **Event Data** - Up to 32 bytes of supplementary information (if available) in hexadecimal format. Event data is described in [Appendix A, Event Code Tables](#).

The *Open Trunking Re-Route Log* ([Figure 4-3](#)) displays interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed switch. The log stores up to 200 entries, and the most recent entry appears at the top of the log.

Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
5/27/03 12:18 pm	16	5	3	6
5/27/03 12:18 pm	15	4	2	5
5/27/03 11:32 am	16	5	3	6
5/27/03 11:32 am	15	4	2	5
5/27/03 11:31 am	16	5	3	6
5/27/03 11:31 am	15	4	2	5

Figure 4-3 Open Trunking Re-Route Log

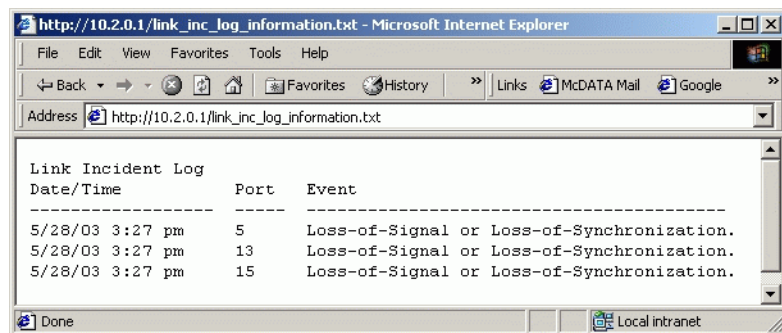
The log consists of the following columns:

- **Date/Time** - Date and time the re-route action occurred.
- **Receive Port** - The switch port number (decimal) used for receiving Fibre Channel traffic after the re-route action.
- **Target Domain** - The domain ID (decimal) of the target device to which Fibre Channel traffic from the switch was rerouted.

- **Old Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic before the re-route action.
- **New Exit Port** - The switch port number (decimal) used for transmitting Fibre Channel traffic after the re-route action.

Link Incident Log

The *Link Incident Log* (Figure 4-4) displays Fibre Channel link incident events recorded at the SANpilot interface. Entries reflect the cause of the link incident. The log stores up to 200 entries, and the most recent entry appears at the top of the log.



Link Incident Log		
Date/Time	Port	Event
5/28/03 3:27 pm	5	Loss-of-Signal or Loss-of-Synchronization.
5/28/03 3:27 pm	13	Loss-of-Signal or Loss-of-Synchronization.
5/28/03 3:27 pm	15	Loss-of-Signal or Loss-of-Synchronization.

Figure 4-4 Link Incident Log

The log consists of the following columns:

- **Date/Time** - Date and time the link incident occurred.
- **Port** - Port number (0 through 11) that reported the link incident.
- **Event** - Brief description of the link incident. Problem descriptions include:
 - Implicit incident.
 - Bit-error threshold exceeded.
 - Loss of signal or loss of synchronization.
 - Not-operational primitive sequence received.
 - Primitive sequence timeout.
 - Invalid primitive sequence received for current link state.

Refer to *MAP 0500: Port Failure and Link Incident Analysis* on page 3-35 for corrective actions in response to these link incident messages.

Viewing the Security Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Security Log* link. The Security Log displays in text format, as shown in [Figure 4-5](#). The log displays in a separate browser window. Close the browser window to close the log.

The security log provides:

- Reason: The reason code for the security Event
- Date/Time: The date/time when the event occurred.
- Trigger Level: The trigger level of the event. Possible values include: Informational, Security Change, or Error
- Count: A cumulative count of events within a known period.
- Category: The event category message with possible values may be: Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved
- Description: Description of the event.
- Data: Any extra or event specific data.

```
Security Log
Reason  Date/Time      Trigger Level      Count
-----
10000   09/30/2004 11:47:12   Informational      1
Category: Successful Connection
Description: EMS User Connected
Data:      User name = 'Administrator' IP address = 127.000.000.001 Role =
          administrator Protocol = http
10400   09/30/2004 11:47:05   Error              1
Category: Authentication Failure
Description: EMS Wrong User Name - Password Combination
Data:      User name = 'Administrator' IP address = 127.000.000.001
10000   09/30/2004 11:46:59   Informational      1
Category: Successful Connection
Description: EMS User Connected
Data:      User name = 'Administrator' IP address = 127.000.000.001 Role =
          administrator Protocol = http
```

Figure 4-5 Security Log

Clearing the Security Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

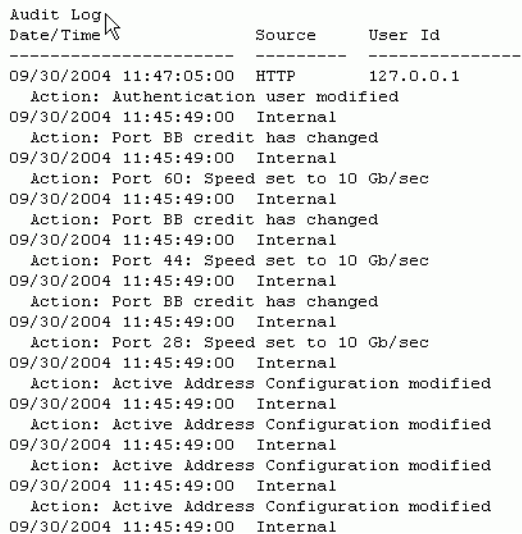
To clear the Security Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Security Log link. A message displays stating that the operation has been performed successfully.

Viewing the Audit Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Audit Log* link. The Audit Log displays in text format, as shown in [Figure 4-6](#). The log displays in a separate browser window. Close the browser window to close the log.

The audit lot provides:

- Date/Time: The date and time of the log entry.
- Source: The source of Audit Log event.
- User ID: Identifier of the user that issued the command. The identifier is usually an IP Address.
- Action: The type of Audit Log event.



A screenshot of a web browser window displaying the 'Audit Log' page. The page has a title bar and a mouse cursor pointing at the 'Audit Log' link. The log is presented as a text-based table with three columns: 'Date/Time', 'Source', and 'User Id'. The data is organized into pairs of rows, where the first row of each pair contains the date, time, source, and user ID, and the second row contains the specific action taken. The log entries are dated 09/30/2004 at 11:45:49:00 and 11:47:05:00. The sources are 'HTTP' and 'Internal'. The user ID for the HTTP entry is '127.0.0.1'. The actions include 'Authentication user modified', 'Port BB credit has changed', 'Port 60: Speed set to 10 Gb/sec', 'Port 44: Speed set to 10 Gb/sec', 'Port 28: Speed set to 10 Gb/sec', and 'Active Address Configuration modified'.

Date/Time	Source	User Id
09/30/2004 11:47:05:00	HTTP	127.0.0.1
Action: Authentication user modified		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 60: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 44: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Port BB credit has changed		
09/30/2004 11:45:49:00	Internal	
Action: Port 28: Speed set to 10 Gb/sec		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	
Action: Active Address Configuration modified		
09/30/2004 11:45:49:00	Internal	

Figure 4-6 Viewing the Audit Log

Clearing the Audit Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Audit Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Audit Log link. A message displays stating that the operation has been performed successfully.

Viewing the Fabric Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Fabric Log*, either a wrapped or non-wrapped view. The Fabric Log displays in text format, as shown in Figure 4-7. The log displays in a separate browser window. Close the browser window to close the log.

TIP: The same entries will go into both logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

The Fabric Log provides:

- **Count:** A cumulative count of entries within a known period.
- **Date/Time:** The date and time of the log entry.
- **Description:** A description of the log entry.
- **Data:** Extended data that is associated with the log entry.

```
Non-Wrapping Fabric Log
Count      Date/Time
-----
10         09/30/2004 11:46:03
  Description: Fabric Operational
  Data:
9          09/30/2004 11:46:03
  Description: Paths Operational
  Data:
8          09/30/2004 11:46:03
  Description: Zone Merge Completed
  Data:
7          09/30/2004 11:46:03
  Description: Notified by Fabric controller and discover new or changed E_Port
              to start zone merge
  Data:
6          09/30/2004 11:46:03
  Description: Path Selection Completed
  Data:
5          09/30/2004 11:46:03
  Description: Domain ID Change
  Data:      New Domain ID=0001, Preferred Domain ID=0001
```

Figure 4-7 Viewing the Fabric Log

Clearing the Fabric Log

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Fabric Log, select *Monitor* and select the *Logs* tab. Select the *Clear Log* button, next to the Fabric Log link. A message displays stating that the operation has been performed successfully.

Viewing the Embedded Port Frame Log

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *Embedded Port Frame Log* link either a wrapped or non-wrapped view. The Frame Logs listing displays in text format, as shown in [Figure 4-10](#). The log displays in a separate browser window. Close the browser window to close the log.

TIP: The same entries will go into both logs until the non-wrap log gets full. Once the non-wrap log gets full, the entries go into the wrap log. Once the wrap log is full, it will start to overwrite entries. If you need to look at a history of log entries, you should review both logs.

The Embedded Port Frame Log provides:

- Count: A cumulative count of entries within a known period.
- Date/- Time: Time of the frame.
- Port #: The port number.
- Direction: Direction of the frame through the port (I = In, O = Out).
- SOF: Start of frame.
- EOF: End of frame.
- Header: The 24 byte FC frame header.
- Payload Size: Size of the payload.
- Payload: The first 32 bytes of the FC frame payload.

Non-Wrapping Embedded Port Frame Log							
Count	Date/Time	Port #	Direction	SOF	EOF	Payload Size	
7	02/02/2004 10:48:20	13	O	f	t	0	
Header: C0FFFFFFD C0FFFFFFD 00580000 01000000 00000001 00000001							
Payload:							
6	02/02/2004 10:48:20	13	I	f	t	0	
Header: C0FFFFFFD C0FFFFFFD 00580000 01000000 00000001 00000001							
Payload:							
5	02/02/2004 10:48:20	13	O	f	n	8	
Header: 03FFFFFFD C0FFFFFFD 22980000 01000000 00000001 00000000							
Payload: 01000000 C0FF0100							
4	02/02/2004 10:48:20	13	I	f	n	8	
Header: 03FFFFFFD C0FFFFFFD 22980000 01000000 00000001 00000000							
Payload: 01000000 C0FF0100							

Figure 4-8 Viewing the Frame Log

Defining Filtering Settings

You can turn on filtering of Class F Frames and to choose which port to filter on. The settings take affect the way entries are added to the log, but do not affect the existing entries in the log. To define the settings, select the *Settings* button.

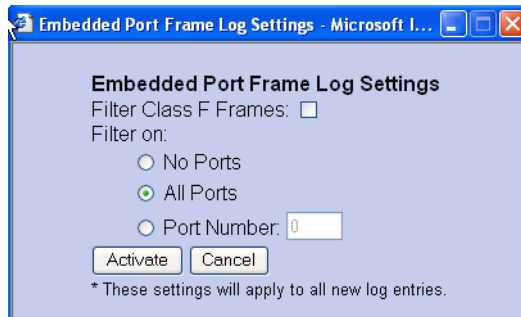


Figure 4-9 Setting Embedded Port Frame Filtering

Clearing Embedded Port Frame Log Entries

ATTENTION! Before clearing logs, make sure the logs are not needed for troubleshooting. Once a log is cleared, the data cannot be retrieved.

To clear the Embedded Frame Log, select *Monitor* and select the *Logs* tab and then select the *Clear Log* button. A message displays stating that the operation has been performed successfully.

Viewing All Logs

Select *Monitor* on the navigation panel. Select the *Logs* tab; the *Logs* tab view displays. Select the *All Logs* link. The All Logs listing displays in text format, as shown in [Figure 4-10](#). The log displays in a separate browser window. Close the browser window to close the log.

Event Log				
Date/Time	Error Code	Severity	Event Data	
4/26/04 4:38 pm	584	Major	17FF FFFF C3C8 0400 0AE7 1DFC FFFF FFFF FFFF FFFF FFFF	
4/26/04 4:38 pm	584	Major	0FFF FFFF B8C8 0400 0A67 DEC1 FFFF FFFF FFFF FFFF FFFF	
4/26/04 4:34 pm	422	Informational		
4/26/04 4:33 pm	417	Informational	3036 2E30 322E 3030 2031 3800 0000 0000 00	
4/26/04 4:33 pm	410	Informational	44	
4/26/04 4:33 pm	421	Informational	3036 2E30 322E 3030 2031 3800 0000 0000 00	
4/26/04 4:32 pm	423	Informational		
Open Trunking Re-Route Log				
Date/Time	Receive Port	Target Domain	Old Exit Port	New Exit Port
4/26/04 4:47 pm	15	27	0	1
4/26/04 4:43 pm	15	27	0	1
Link Incident Log				
Date/Time	Port	Link Incident Event		
4/26/04 4:38 pm	23	Not Operational primitive sequence (NOS) received.		
4/26/04 4:38 pm	15	Not Operational primitive sequence (NOS) received.		

Figure 4-10 All Logs View

The **All Logs** listing provides the ability to view (display) all of the content of the logs.

Clearing All Log Entries

ATTENTION! Before clearing information in all of the logs, make sure the logs are not needed for troubleshooting. Once the logs are cleared, the data cannot be retrieved.

To clear all logs' entries, select *Monitor* and select the *Logs* tab. Select the *Clear All Logs* button, next to the All Logs link. A message displays stating that the operation has been performed

Obtain Port Diagnostic Information

Fibre Channel port diagnostic information can be obtained by inspecting port LEDs at the switch front panel or operating parameters at the SANpilot interface.

Port LEDs

To obtain port operational information, inspect port LEDs at the switch front panel. Amber and blue/green LEDs adjacent to each port indicate operational status as described in [Table 4-1](#).

Table 4-1 Port Operational States

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Inactive	On	Off	Yellow Triangle	The port is inactive. The reason appears in the <i>Reason</i> field at the <i>Port Properties</i> dialog box.
Not Installed	Off	Off	None	An optical transceiver is not installed in the switch port.
Not Operational	Off	Off	Yellow Triangle	The port is receiving the not operational sequence (NOS) from an attached device.
Offline	Off	Off	None	The port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	Yellow Triangle	The port is unblocked and receiving the OLS, indicating the attached device is offline.
Online	On or Blinking	Off	None	An attached device is connected to the switch and ready to communicate, or is communicating through the switch with other attached devices.
				If the port remains online at 1.0625 Gbps, the blue/green LED illuminates green. If the port remains online at 2.125 Gbps, the blue/green LED illuminates blue.
				At the switch, the blue/green LED blinks green when there is Fibre Channel traffic through the port at 1.0625 Gbps. At the switch, the blue/green LED blinks blue when there is Fibre Channel traffic through the port at 12.125 Gbps.
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	Yellow Triangle	The port has an invalid attachment. The reason appears in the <i>Reason</i> field at the <i>Port Properties</i> dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred. The alert symbol appears at the <i>Hardware View</i> and <i>Port List View</i> .
Link Reset	Off	Off	Yellow Triangle	The switch and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is received at the switch port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The port failed and requires service.

Table 4-1 Port Operational States (Continued)

Port State	Blue/Green LED	Amber LED	Alert Symbol	Description
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected switches from joining and forming a multiswitch fabric. The reason appears in the <i>Reason</i> field of the <i>Port Properties</i> dialog box.
Testing	Off	Blinking	Yellow Triangle	The port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	The port is performing an external loopback test.

SANpilot Interface

To obtain port operational information at the SANpilot interface, inspect parameters at the:

- *Monitor Panel - Port List* page.
- *Monitor Panel - Port Stats* page.
- *View panel - Port Properties* page.

Port List Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed ([Figure 4-11](#) on page 4-14).

Port #	Name	Block Configuration	State	Type
0		Unblocked	Offline	Fx Port
1		Unblocked	Offline	Fx Port
2		Unblocked	Offline	Fx Port
3		Unblocked	Offline	Fx Port
4		Unblocked	Offline	Fx Port
5		Unblocked	Offline	Fx Port
6		Unblocked	Offline	Fx Port
7		Unblocked	Offline	Fx Port
8		Unblocked	Offline	Fx Port
9		Unblocked	Offline	Fx Port
10		Unblocked	Offline	Fx Port
11		Unblocked	Offline	Fx Port

Figure 4-11 Monitor Panel (Port List Page)

A row of information for each port (0 through 11 inclusive) appears. Each row consists of the following columns:

- **Port #** - Switch port number.
- **Name** - Port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration** - Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the offline sequence (OLS).
- **State** - Port state (*Online, Offline, Not Installed, Inactive, Invalid Attachment, Link Reset, No Light, Not Operational, Port Failure, Segmented E_Port, or Testing*).
- **Type** - Configured port type. Settings are:
 - Generic mixed port (GX_Port). This setting also configures a port as a generic loop port (GL_Port). This selection is available only if enabled through an optional product feature enablement (PFE) key.

- Fabric mixed port (FX_Port). This setting also configures a port as a fabric loop port (FL_Port).
- Generic port (G_Port). This selection is available only if enabled through an optional PFE key.
- Fabric port (F_Port).
- Expansion port (E_Port). This selection is available only if enabled through an optional PFE key.

Port Stats Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed. Click the *Port Stats* tab. The *Monitor* panel displays with the *Port Stats* page selected (Figure 4-12).

Monitor: Refresh-5 / 27 / 03 at 12:21:41

Port List Port Stats Logs Node List

Port Number: 0 Get Port Statistics << Back Fwd >>

Clear Port Statistics Clear All Port Stats

Statistics Values for PORT 0

Traffic Statistics	# of Wraps	Counter
Frames Rx	0	0
Frames Tx	0	0
Four byte words Rx	0	0
Four byte words Tx	0	0
Offline sequences Rx		7098
Offline sequences Tx		7208
Link resets Rx		7249
Link resets Tx		7267
LIPs Detected		7269
LIPs Generated		7493
Link utilization % Rx		0
Link utilization % Tx		0

Figure 4-12 Monitor Panel (Port Stats Page)

The *Port Stats* page displays traffic and error statistics for one port. Values update only when the page opens for a selected port or the user selects *Get Port Statistics*. The page defaults to port 0. Increment or decrement the port number displayed (0 through 11 inclusive) by clicking *Fwd>>* or *<<Back*.

The *# of Wraps* column tracks the number of times the counter wraps for rapidly-growing statistics. The maximum counter value is 2^{32} entries. The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Traffic statistics** - These entries provide information about port traffic, including:
 - Fibre Channel frames received and transmitted.
 - Four-byte words received and transmitted.
 - Offline sequences received and transmitted.
 - Link resets received and transmitted.
 - Loop initialization primitives (LIPs) generated and detected.
 - Percent link utilization (receive and transmit).
- **Error statistics** - The *Port Stats* page displays the following error statistics for the port:
 - **Link failures** - Link failures are recorded in response to a not operational sequence (NOS), protocol timeout, or port failure.
 - **Sync losses** - Synchronization losses are detected because an attached device was reset or disconnected from the port.
 - **Signal losses** - Signal losses are detected because an attached device was reset or disconnected from the port.
 - **Primitive sequence errors** - Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations.
 - **Discarded frames** - Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.
 - **Invalid transmission words** - Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.

- **CRC errors** - Received frames failed cyclic redundancy check (CRC) validation, indicating the frames arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** - Received frames had frame delimiter errors, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Address ID errors** - Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- **Frames too short** - Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Class 2 statistics** - These entries provide information about Class 2 traffic, including:
 - Class 2 frames received and transmitted.
 - Four-byte words received and transmitted.
 - Busied and rejected frames.
- **Class 3 statistics** - These entries provide information about Class 3 traffic, including:
 - Class 3 frames received and transmitted.
 - Four-byte words received and transmitted.
 - Discarded frames.

Port Properties Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, click the *Port Properties* tab. The *View* panel displays with the *Port Properties* page selected (Figure 4-13 on page 4-18).

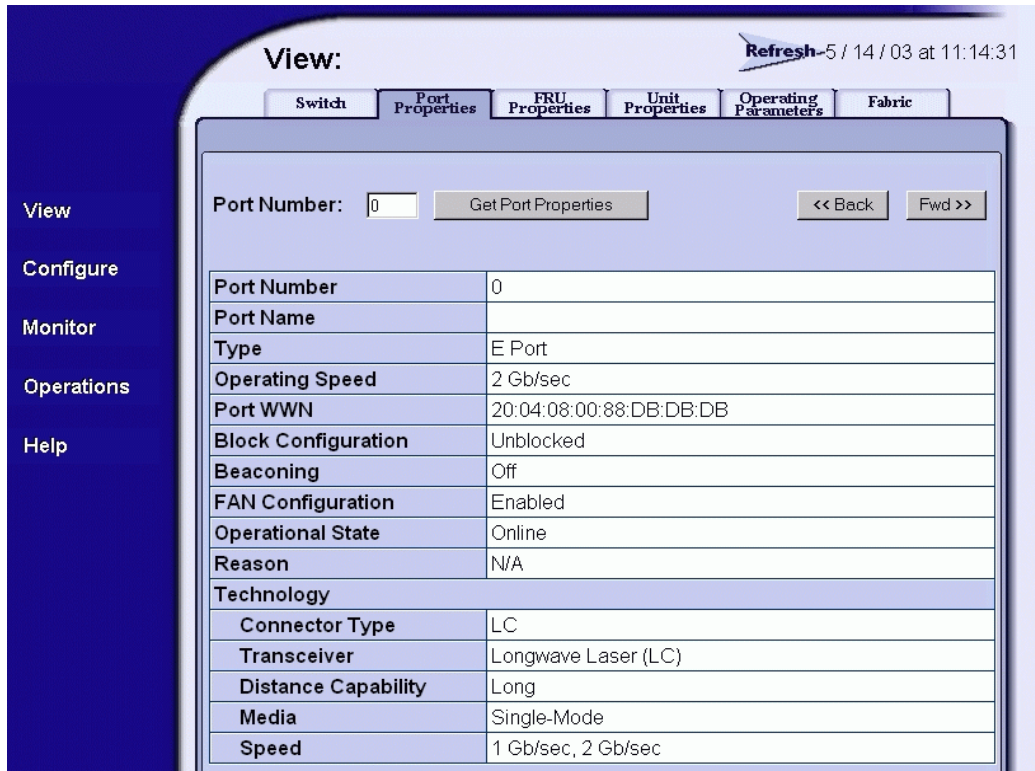


Figure 4-13 View Panel (Port Properties Page)

The *Port Properties* page displays information for one port. Values update only when the page opens for a selected port or the user selects *Get Port Properties*. The page defaults to port 0. Increment or decrement the port number displayed (0 through 11 inclusive) by clicking *Fwd>>* or *<<Back*. The page provides the following information:

- **Port Number** - Switch port number.
- **Port Name** - User-defined name or description for the port.
- **Type** - Port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed** - Operating speed (*Not Established*, *1 Gbps*, or *2 Gbps*).
- **Port WWN** - Fibre Channel world wide name (WWN) for the port.

- **Block Configuration** - User-configured state for the port (*Blocked* or *Unblocked*).
- **Beaconing** - User-specified for the port (*On* or *Off*).
- **FAN Configuration** - User-configured state for fabric address notification (FAN) configuration (*Enabled* or *Disabled*).
- **Operational State** - Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).
- **Reason** - A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason is *N/A*.
- **Technology** - Information specific to the installed optical transceiver, including connector type, transceiver optics, data transmission distance, optical media (cable type), and transmission speed.

Perform Port Diagnostic Loopback Tests

Port diagnostics consist of internal and external loopback tests. The tests are performed on any selected port at the SANpilot interface. The tests are described as follows:

- **Internal loopback test** - An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.
- **External loopback test** - An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Internal Loopback Test

To perform an internal loopback at the SANpilot interface:

1. Notify the customer that a disruptive internal loopback test is to be performed. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port, and sets the attached device offline.

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

2. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
3. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-14).

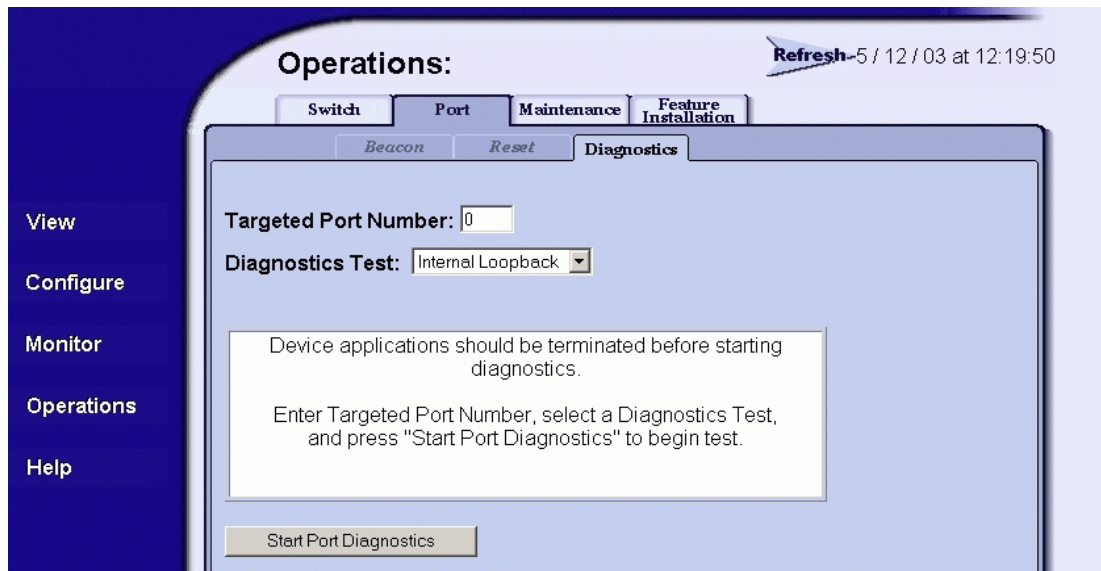


Figure 4-14 Operations Panel (Port Page with Diagnostics Tab)

4. Type the port number to be tested in the *Targeted Port Number* field.
5. At the *Diagnostics Test* list box, select the *Internal Loopback* option.
6. Click *Start Port Diagnostics*. The test begins and:
 - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.

- b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Terminate Port Diagnostics* at any time to abort the loopback test.

7. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.
8. Reset the tested port:
 - a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
 - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
 - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
9. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test

To perform an external loopback at the SANpilot interface:

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. Disconnect the fiber-optic jumper cable from the port to be tested.
3. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
4. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
5. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-14 on page 4-20).
6. Type the port number to be tested in the *Targeted Port Number* field.
7. At the *Diagnostics Test* list box, select the *External Loopback* option.

8. Click *Start Port Diagnostics*. The test begins and:
 - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.
 - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Terminate Port Diagnostics* at any time to abort the loopback test.

9. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in [step 2](#)).
11. Reset the tested port:
 - a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
 - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
 - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
12. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Collect Maintenance Data

When the switch operational firmware detects a critical error, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card. The operator then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the web browser PC hard drive.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by support personnel. Maintenance data includes the dump file and an engineering log viewable only by support personnel.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through the switch's maintenance port, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data (retrieve the dump file from the CTP card) at the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Maintenance* and *System Files* tabs. The *Maintenance* page displays with the *System Files* tab selected (Figure 4-15).

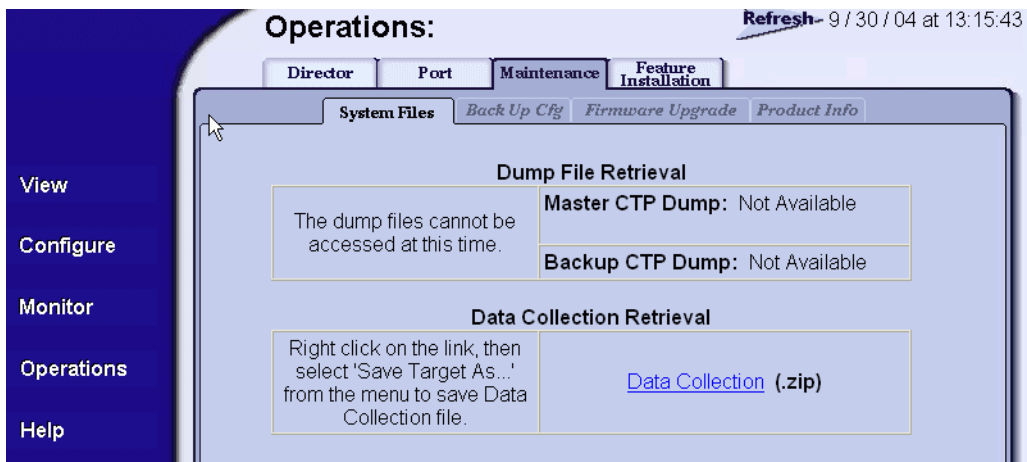


Figure 4-15 Operations Panel (Maintenance Page with System Files Tab)

3. Right-click the *CTP Dump* link to open a list of menu options.
4. Select the *Save Target As* menu option. The *Save As* dialog box displays (Figure 4-16 on page 4-24).

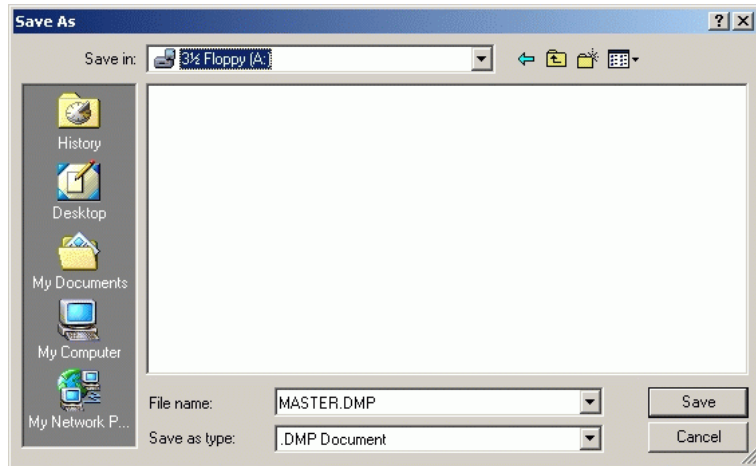


Figure 4-16 Save As Dialog Box

5. Insert a blank diskette in the floppy drive of the browser PC.
6. At the *Save As* dialog box, select the floppy drive (A:\) from the *Save in* drop-down menu, type a descriptive name for the dump file in the *File name* field, and click *Save*.
7. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-17).

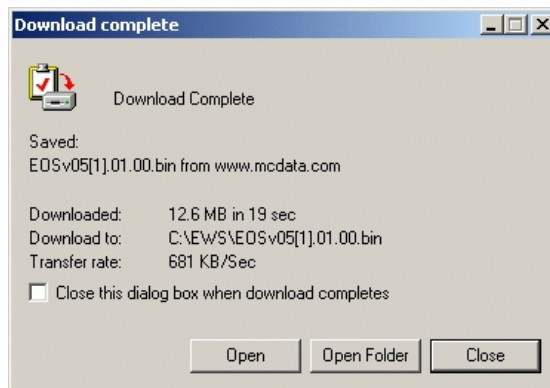


Figure 4-17 Download Complete Dialog Box

8. Click *Close* to close the dialog box.
9. Remove the diskette with the newly-collected maintenance data from the browser PC floppy drive. Return the diskette with the failed FRU to McDATA for failure analysis.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These operating states are described as follows:

- **Online** - When the switch is set online, an attached device can log in to the switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline** - When the switch is set offline, all switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

NOTE: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the switch online from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected ([Figure 4-18](#) on page 4-26).

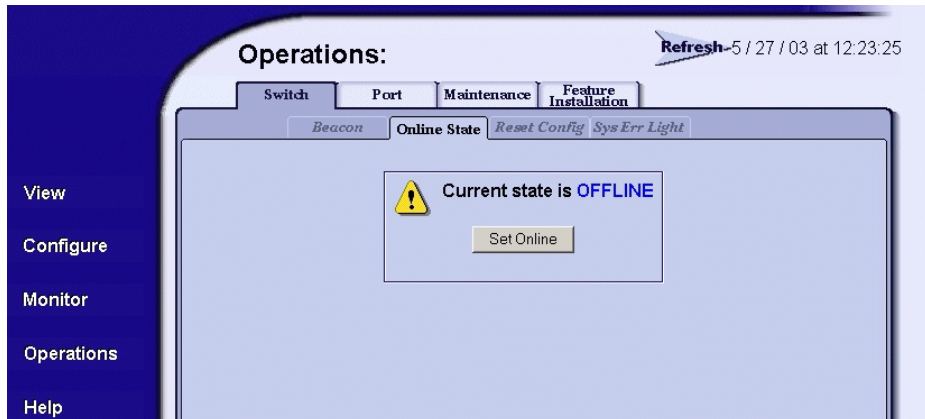


Figure 4-18 Operations Panel (Switch Page with Online State Tab)

3. Click Set Online. The switch comes online and the message **Your changes have been successfully activated** appears.

Set Offline State

To set the switch offline from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected (Figure 4-18).
3. Click Set Offline. The switch goes offline and the message **Your changes have been successfully activated** appears.

Block or Unblock a Port

This section describes procedures to block or unblock a switch Fibre Channel port. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).

Block a Port

To block a switch port from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-19).

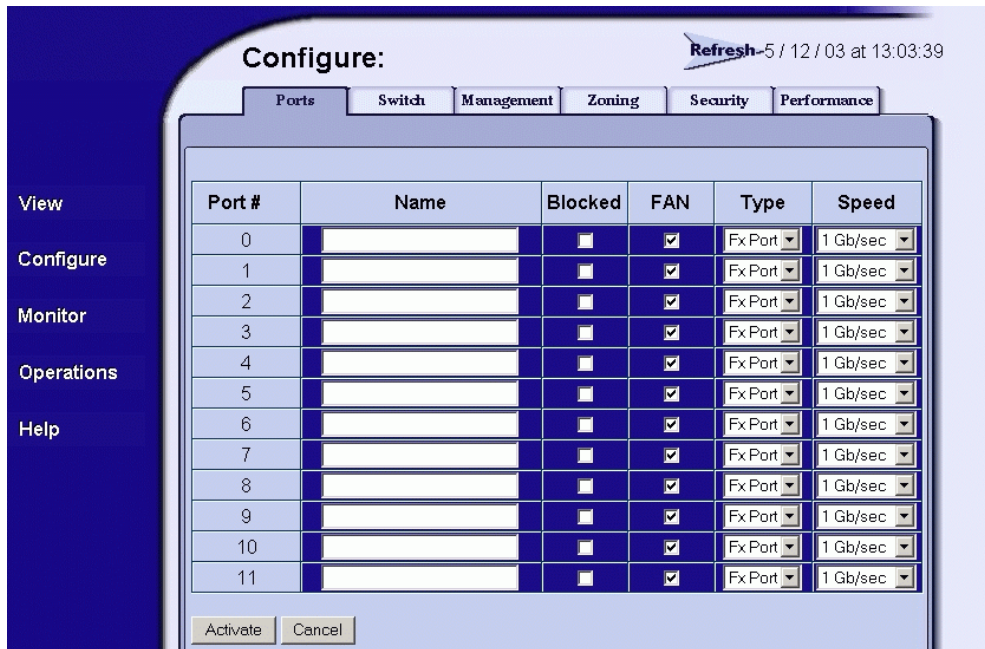


Figure 4-19 Configure Panel (Ports Page)

2. Click the check box for the selected port in the *Blocked* column to block the port (default is unblocked). A check mark in the box indicates the port is blocked.
3. Click *Activate* at the bottom of the page to save and activate the blocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

Unblock a Port

To unblock a switch port from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-19 on page 4-27).
2. Click the check box for the selected port in the *Blocked* column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click *Activate* at the bottom of the page to save and activate the unblocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the transceiver. Use compressed air to blow any contaminants from the connector as shown in part A of Figure 4-20.
 - Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
 - Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

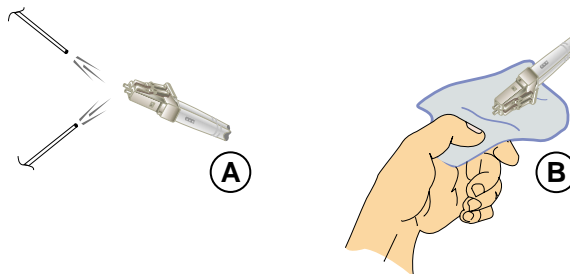


Figure 4-20 Clean Fiber-Optic Components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in part **B** of [Figure 4-20](#) on page 4-28. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
4. Repeat [step 2](#) and [step 3](#) of this procedure (second cleaning).
5. Repeat [step 2](#) and [step 3](#) of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power on the switch:

1. One alternating current (AC) power cord is required for the power supply. Ensure a power cord is available to connect the switch to facility power.



DANGER

Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

2. Plug the power cord into a facility power source and power supply AC connector at the rear of the switch. When the power cord is connected, the switch powers on and performs power-on self-tests (POSTs).
3. During POSTs:
 - The green power (**PWR**) LED on the switch front panel illuminates.
 - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
 - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.

4. After successful POST completion, the green power (**PWR**) LED remains illuminated and all amber LEDs extinguish.
5. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

Power-Off Procedure

To power off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-25.
3. Disconnect the power cord from the power supply AC connector at the rear of the switch.

IML or Reset the Switch

This section describes procedures to IML or reset the Sphereon 4300 Switch. An IML or reset is performed at the switch front panel using the **IML/RESET** button.

An IML does not cause power-on diagnostics to execute and is not disruptive to Fibre Channel traffic. The operation:

- Reloads switch firmware from FLASH memory.
- Resets the Ethernet LAN interface, causing the connection to the web browser PC to drop momentarily until the connection automatically recovers.

A switch reset is more disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the web browser PC to drop momentarily until the connection automatically recovers.

- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

ATTENTION ! A reset should only be performed if a CTP card failure is indicated. Do not reset a managed product unless directed to do so by a procedural step or the next level of support.

Switch IML

To IML the switch from the front panel:

1. Press and hold the **IML/RESET** button until the amber **ERR** LED blinks at twice the unit beaoning rate (approximately three seconds).
2. Release the button to IML the switch. During the IML, the switch-to-PC Ethernet link drops momentarily.

Switch Reset

To reset the switch from the front panel:

1. Press and hold the **IML/RESET** button for approximately ten seconds.
 - After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaoning rate.
 - After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
 - The green power (**PWR**) LED on the switch front panel illuminates.
 - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
 - The green LED associated with the Ethernet port blinks momentarily while the port is tested.
 - The blue/green and amber LEDs associated with the ports blink momentarily while the ports are tested.
 - The switch-to-PC Ethernet link drops momentarily.

Manage Firmware Versions

Firmware is the switch operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a browser PC hard drive and made available for download to the switch from the SANpilot interface.

Service personnel can perform the following firmware management tasks from the SANpilot interface:

- Determine the firmware version actively running on the switch.
- Add a firmware versions to the browser PC hard drive.
- Download a firmware version to the switch.

Determine Switch Firmware Version

To determine a switch firmware version from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, click the *Unit Properties* tab. The *Unit Properties* page displays ([Figure 4-21](#)).

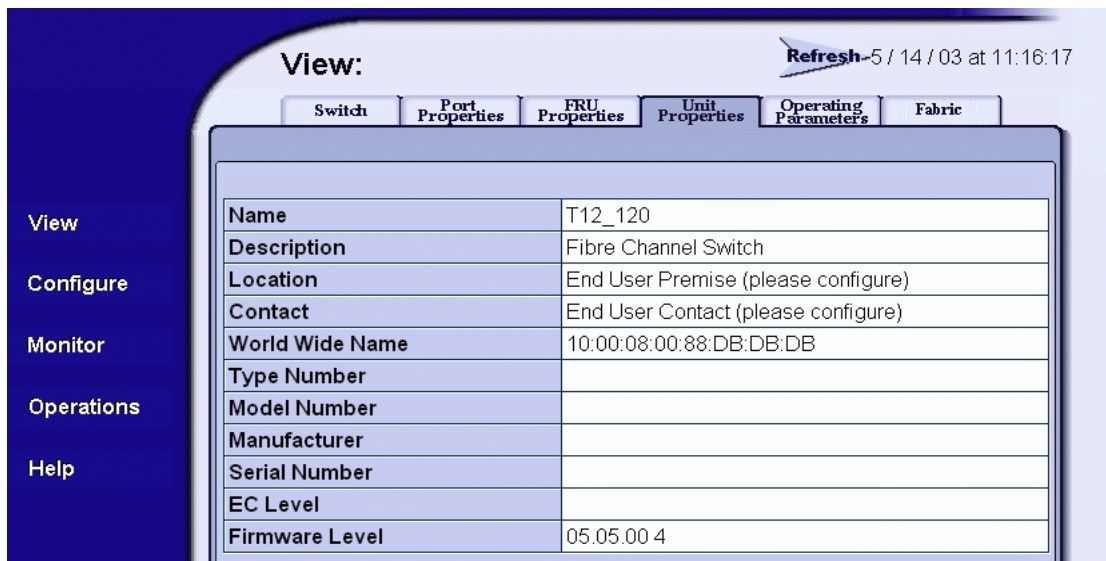


Figure 4-21 View Panel (Unit Properties Page)

Add a Firmware Version to the Browser PC Hard Drive

2. At the bottom of the page, record the firmware version listed in the *Firmware Level* field.

The firmware version shipped with the switch is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent firmware versions for upgrading the switch are provided to customers through McDATA's Internet home page.

NOTE: When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the code. This information supplements information provided in this general procedure.

To add a switch firmware version to the browser PC hard drive (PC running the SANpilot interface):

1. Obtain the new firmware version from the McDATA File Center. At a PC with Internet access, open the File Center home page (Figure 4-22). The uniform resource locator (URL) is <http://central.mcddata.com>.

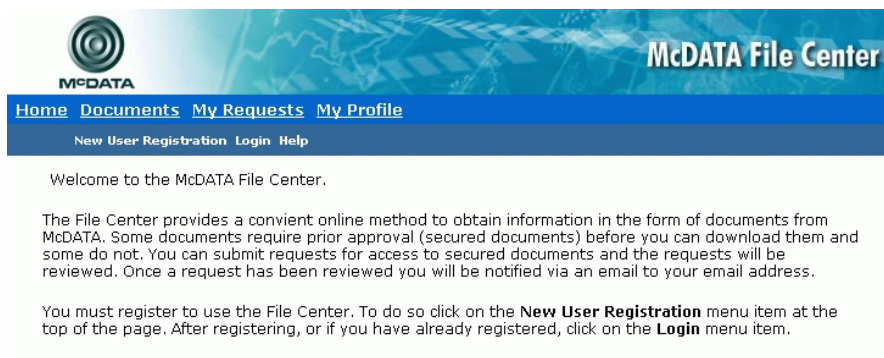
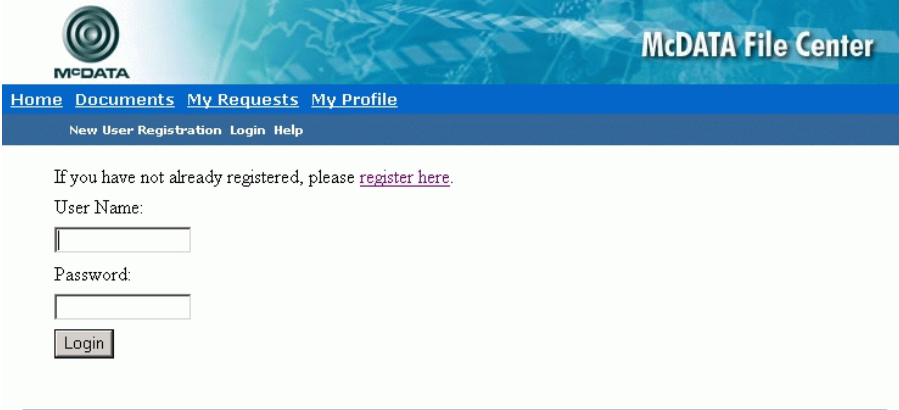


Figure 4-22 McDATA File Center Home Page

2. Select (click) the *Login* option at the top of the home page. The *Login* page displays (Figure 4-23 on page 4-34).



The login page features the McDATA logo and a navigation bar with links: Home, Documents, My Requests, and My Profile. Below the navigation bar are links for New User Registration, Login, and Help. The main content area includes a registration prompt, a User Name input field, a Password input field, and a Login button.

McDATA File Center

Home Documents My Requests My Profile

New User Registration Login Help

If you have not already registered, please [register here](#).

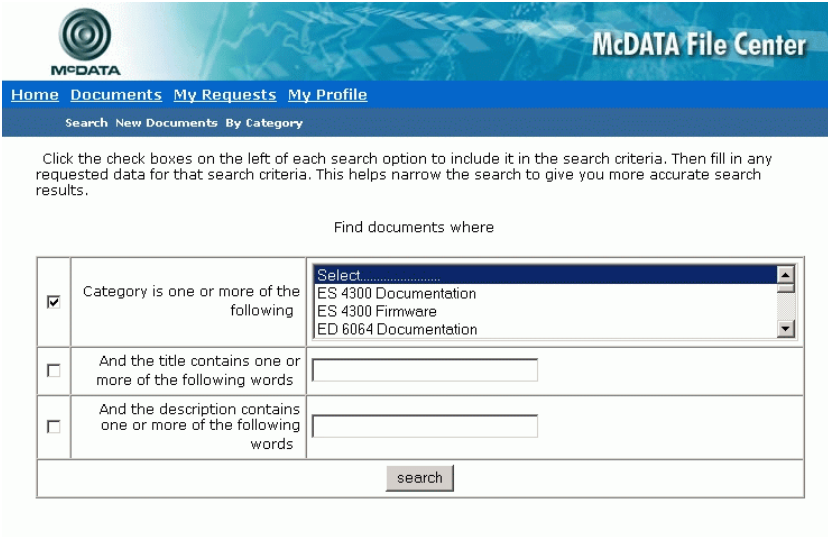
User Name:

Password:

Login

Figure 4-23 McDATA File Center (Login Page)

3. Type the user name and password (assigned and registered while performing *Task 8: Register with the McDATA File Center* on page 2-52) and click *Login*. The *Welcome* page displays.
4. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays (*Figure 4-24*).



The Find Documents page features the McDATA logo and a navigation bar with links: Home, Documents, My Requests, and My Profile. Below the navigation bar are links for Search, New Documents, and By Category. The main content area includes a search instruction, a search criteria table, and a search button.

McDATA File Center

Home Documents My Requests My Profile

Search New Documents By Category

Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.

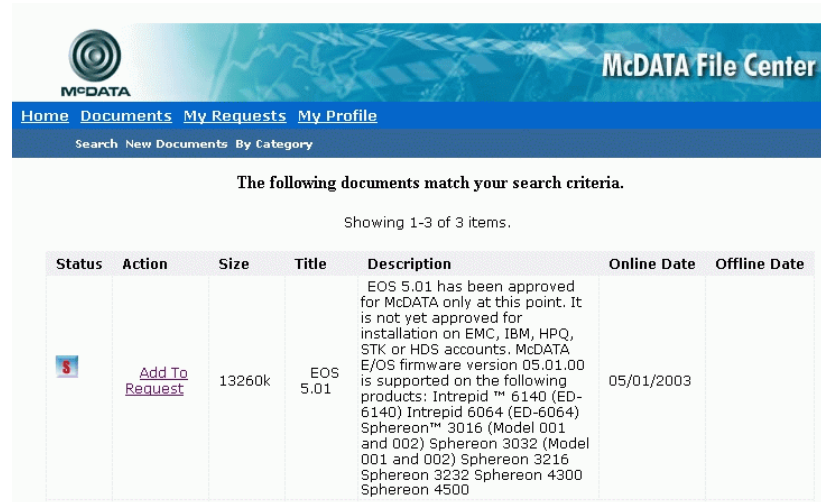
Find documents where

<input checked="" type="checkbox"/>	Category is one or more of the following	Select..... ES 4300 Documentation ES 4300 Firmware ED 6064 Documentation
<input type="checkbox"/>	And the title contains one or more of the following words	
<input type="checkbox"/>	And the description contains one or more of the following words	

search

Figure 4-24 McDATA File Center (Find Documents Page)

- Select (highlight) the *ES 4300 Firmware* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-25) with a list of firmware available for download.



The screenshot shows the McDATA File Center interface. The header includes the McDATA logo and the text "McDATA File Center". Below the header is a navigation bar with links: Home, Documents, My Requests, and My Profile. A search bar is also present. The main content area displays the message "The following documents match your search criteria." and "Showing 1-3 of 3 items." Below this is a table with the following data:


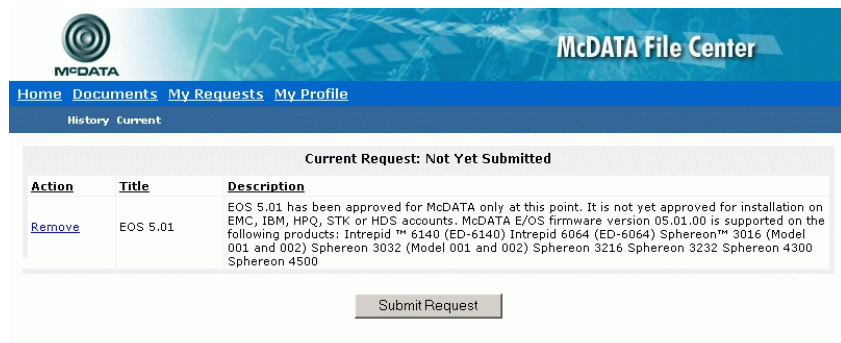
Status	Action	Size	Title	Description	Online Date	Offline Date
	Add To Request	13260k	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4300 Sphereon 4500	05/01/2003	

Figure 4-25 McDATA File Center (Documents Match Page)

- Authorization to download a firmware version typically requires approval from the McDATA solution center. In the *Action* column adjacent to the desired firmware version, click *Add to Request*. The *Current Request* page displays (Figure 4-26).



The screenshot shows the McDATA File Center interface. The header includes the McDATA logo and the text "McDATA File Center". Below the header is a navigation bar with links: Home, Documents, My Requests, and My Profile. A sub-navigation bar shows "History" and "Current". The main content area displays the message "Current Request: Not Yet Submitted". Below this is a table with the following data:

Action	Title	Description
Remove	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4300 Sphereon 4500

Below the table is a button labeled "Submit Request".

Figure 4-26 McDATA File Center (Current Request Page)

- Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA solution center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-27) with the approved request.

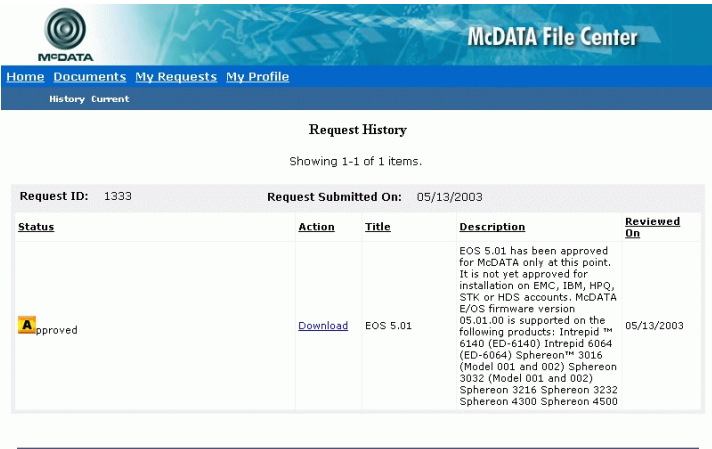


Figure 4-27 McDATA File Center (Request History Page)

- In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays (Figure 4-28).

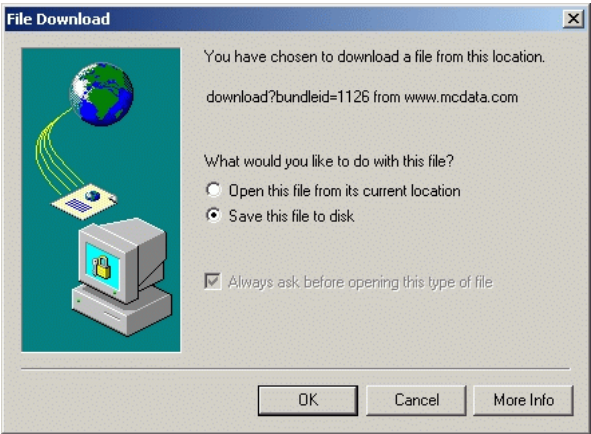


Figure 4-28 File Download Dialog Box

9. Select the *Save this file to disk* radio button and click OK. The *Save As* dialog box appears (Figure 4-29).

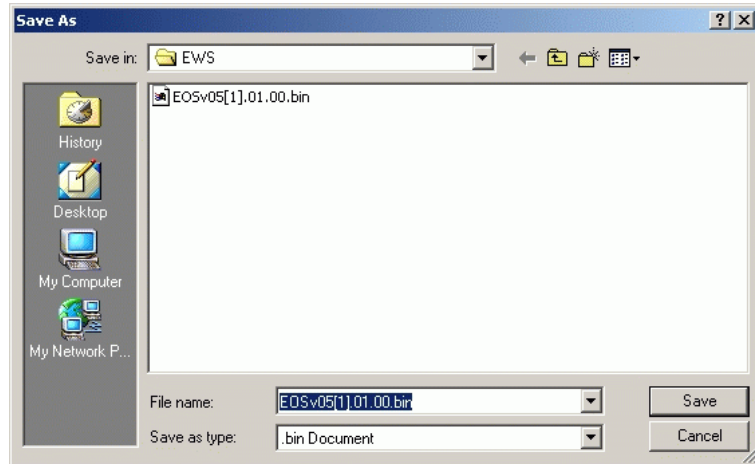


Figure 4-29 Save As Dialog Box

10. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
11. A *Download* dialog box displays, showing the estimated time remaining to complete the download process. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-30).

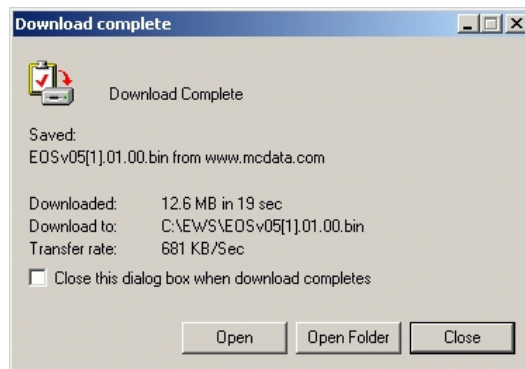


Figure 4-30 Download Complete Dialog Box

12. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the browser PC hard drive.
13. At the browser PC, close the Internet session.

Download a Firmware Version to the Switch

To download a firmware version (to the switch) from the hard drive of the browser PC accessing the SANpilot interface:

NOTE: When downloading a firmware version, follow all procedural information contained in release notes or EC instructions that accompany the firmware version. This information supplements information provided in this general procedure.

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Maintenance* and *Firmware Upgrade* tabs. The *Maintenance* page displays with the *Firmware Upgrade* tab selected (Figure 4-31).

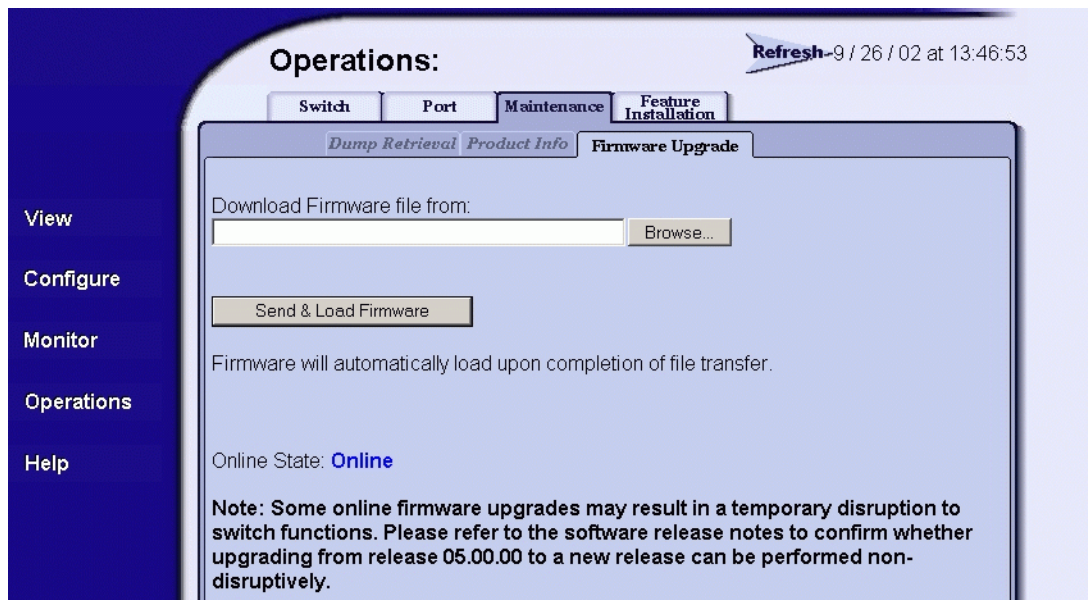


Figure 4-31 Operations Panel (Maintenance Page with Firmware Upgrade Tab)

3. At the *Download Firmware file from* field:
 - Select the desired firmware file from the PC hard drive using the *Browse* button, or
 - Type the desired firmware filename in the *Download Firmware file from* field.
4. Click *Send and Load Firmware*. A browser-specific message box displays (Figure 4-32).

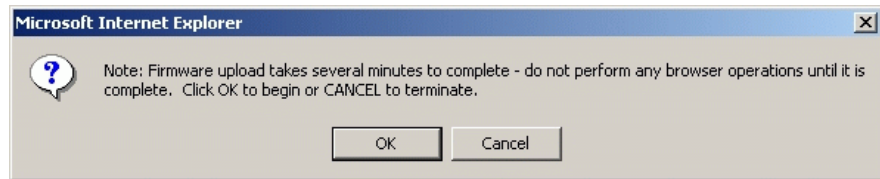


Figure 4-32 Browser-Specific Message Box

5. Click *OK* to download the firmware version to the switch. The download process takes several minutes to complete, during which the browser is unavailable.
6. When the firmware version is downloaded to the switch and verified, the following message box displays (Figure 4-33).

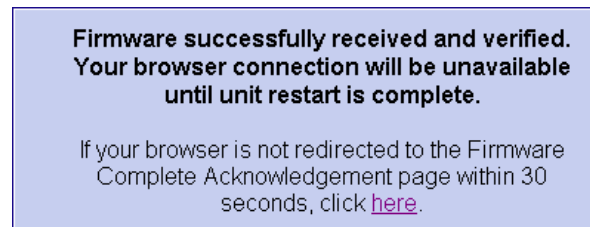


Figure 4-33 Firmware Received Message Box

7. After firmware verification, the switch performs an IML that takes approximately 30 seconds to complete. During the IML, the browser-to-switch Internet connection drops momentarily and the SANpilot session is lost.
8. After the switch IML and SANpilot session logout, the following message box displays (Figure 4-34 on page 4-40).



Figure 4-34 Firmware Upgrade Complete Message Box

9. Click [here](#) to login to the switch and start a new SANpilot session. The *Enter Network Password* dialog box displays.
10. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

11. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed.

Reset Configuration Data

The SANpilot interface provides the option to reset the configuration file to factory default values. The switch must be set offline prior to restoring the configuration file. Configuration data in the file include:

- Switch identification data.
- Port configuration data.
- Switch and fabric operating parameters.
- Simple network management protocol (SNMP) configuration information.
- Zoning configuration information.

To reset switch data to the factory default settings from the SANpilot interface:

NOTE: When switch configuration data is reset to factory default values, all optional features are disabled.

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.
2. Set the switch offline. For instructions, refer to [Set the Switch Online or Offline](#) on page 4-25.
3. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
4. Click the *Reset Config* tab. The *Switch* page displays with the *Reset Config* tab selected ([Figure 4-35](#)).

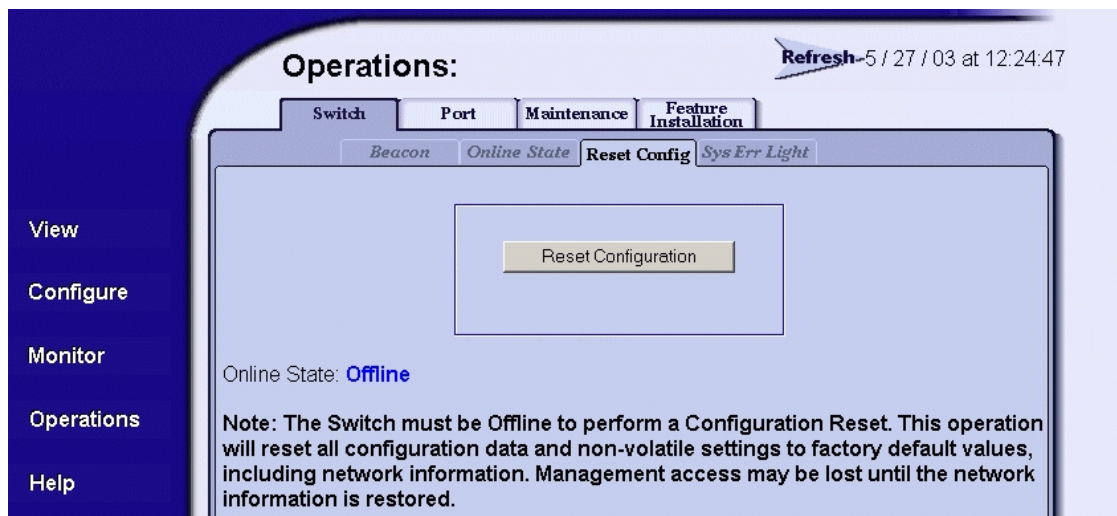


Figure 4-35 Operations Panel (Switch Page with Reset Config Tab)

5. Click *Reset Configuration*. A browser-specific message box displays ([Figure 4-36](#) on page 4-42).

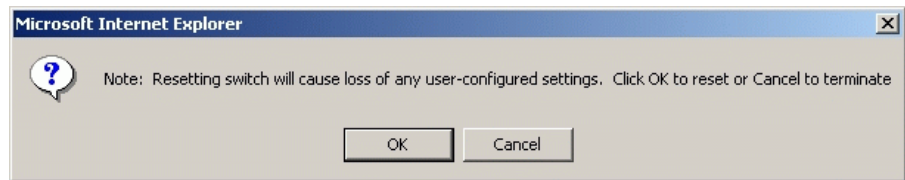


Figure 4-36 Browser-Specific Message Box

6. Click *OK* to reset the configuration. The message **Your changes have been successfully activated** appears.
7. The switch IP address resets to the default address of **10.1.1.10**.
 - If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Internet connection is not affected and the procedure is complete.
 - If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Internet connection drops and the SANpilot session is lost. Continue to the next step.
8. To change the switch IP address and restart the SANpilot interface, refer to [Configure Network Information](#) on page 2-19. To restart the SANpilot interface using the default IP address of **10.1.1.10**:
 - a. At the browser, enter the default IP address of **10.1.1.10** as the Internet uniform resource locator (URL). The *Enter Network Password* dialog box displays.
 - b. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- c. Click *OK*. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed. The procedure is complete.

This chapter describes removal and replacement procedures (RRPs) used by authorized service representatives for all Sphereon 4300 Switch field-replaceable units (FRUs). Do not remove a switch FRU until a failure is isolated to that FRU. If fault isolation was not performed, refer to *MAP 0000: Start MAP* on page 3-6.

Procedural Notes

The following procedural notes are referenced in applicable removal and replacement procedures.

1. Before removing a FRU, read the removal and replacement procedures for that FRU carefully and thoroughly to familiarize yourself with the procedures and reduce the possibility of problems or customer down time.
2. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
3. After completing a replacement procedure, clear the event code reporting the failure and the event code reporting the recovery from the *Event Log* at the SANpilot interface, and extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

RRP 1: SFP Optical Transceiver

Small form factor pluggable (SFP) optical transceivers are the only concurrent FRUs removed and replaced while the switch is powered on and operational. The FRU has no ESD precaution requirements.

Use the following procedures to remove or replace an SFP optical transceiver from the front of the switch chassis. A list of tools required is provided. Refer to [Chapter 6, *Illustrated Parts Breakdown*](#) for FRU locations and part numbers.

Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabriccenter equipment cabinet).
- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the switch).
- Fiber-optic cleaning kit.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. If the switch is installed as part of a stand-alone configuration, go to [step 3](#). If the switch is rack-mounted, perform one of the following:
 - If the switch is installed in a McDATA FC-512 Fabriccenter equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door.
 - If the switch is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative.
3. Identify the defective port transceiver from:
 - The illuminated amber LED adjacent to the port.
 - At the SANpilot interface, failure information associated with the port at the *Port Properties* page of the *View* panel.

4. Block communication to the port. Refer to [Block or Unblock a Port](#) on page 4-26 for instructions.
5. Disconnect the fiber-optic jumper cable from the port:
 - a. Pull the keyed LC connector free from the port's optical transceiver.
 - b. Place a protective cap over the jumper cable connector.
6. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The locking bale rotates up or down, depending on the transceiver manufacturer and port location (top row, odd-numbered ports **1** through **11**, or bottom row even-numbered ports **0** through **10**).
 - a. Disengage the locking mechanism by rotating the wire locking bale up or down 90 degrees as shown in part (A) of [Figure 5-1](#).



Figure 5-1 SFP Optical Transceiver Removal and Replacement

- b. Grasp the wire locking bale and pull the transceiver from the port receptacle as shown in part (B) of [Figure 5-1](#) on page 5-3.
- c. At the web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. An event code **513** (SFP optics hot-removal completed) appears in the log.

Replacement

To replace an SFP optical transceiver:

1. Remove the replacement transceiver from its packaging.
2. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire locking bale up or down 90 degrees as shown in [Figure 5-1](#) on page 5-3.
3. Perform an external loopback test on the port. Refer to [Perform Port Diagnostic Loopback Tests](#) on page 4-19 for instructions. If the test fails, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
 - a. Remove the protective cap from the cable connector and the protective plug from the port's optical transceiver. Store the cap and plug in a suitable location for safekeeping.
 - b. Clean the jumper cable and transceiver connectors. Refer to [Clean Fiber-Optic Components](#) on page 4-28 for instructions.
 - c. Insert the keyed LC cable connector into the port's optical transceiver.
5. Ensure the amber LED adjacent to the port transceiver is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
6. At the web browser connected to the SANpilot interface, click the *Log* tab at the *Monitor* panel. The *Event Log* displays. Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.

7. Open the *Switch* tab at the *View* panel and:
 - a. Ensure no amber LEDs illuminate that indicate a port failure.
 - b. Click the graphic representing the port with the replacement transceiver to open the *Port Properties* tab. Verify port and port technology information is correct.
 - c. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-6 to isolate the problem.
8. Restore communication to the port with the replacement transceiver as directed by the customer. Refer to [Block or Unblock a Port](#) on page 4-26 for instructions. Inform the customer the port is available.
9. To clear the system error (**ERR**) LED on the switch front bezel from the web browser connected to the SANpilot interface:
 - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
 - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
 - c. Click *Clear Light*.
10. If necessary, close and lock the equipment cabinet door.

This chapter provides an illustrated parts breakdown for Sphereon 4300 Switch field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the switch disassembly sequence for clarity. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include McDATA part numbers, descriptions, and quantities.

Front-Accessible FRUs

Figure 6-1 illustrates front-accessible FRUs. Table 6-1 is the associated FRU parts list. The table includes reference numbers to Figure 6-1, FRU part numbers, descriptions, and quantities.

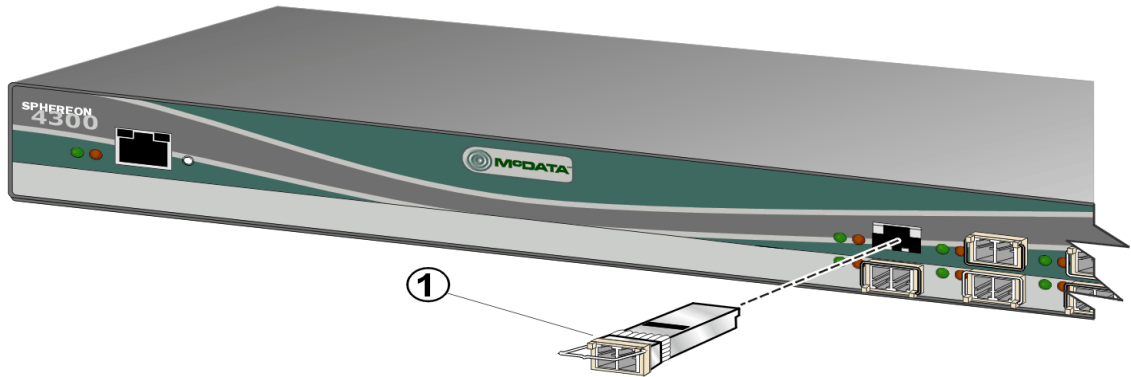


Figure 6-1 Front-Accessible FRUs

Table 6-1 Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6-1	002-002688-100	Switch, Sphereon 4300, base assembly	Reference
-1	803-000054-395	Transceiver, optical, SFP, shortwave laser, LC connector, 1.0625 Gbps	0 to 12
-1	803-000064-395	Transceiver, optical, SFP, shortwave laser, LC connector, 2.125 Gbps	0 to 12
-1	803-000056-313	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 1.0625 Gbps	0 to 12
-1	803-000065-313	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 2.125 Gbps	0 to 12
-1	803-000066-313	Transceiver, optical, SFP, longwave laser, LC connector, 20 km, 2.125 Gbps	0 to 12
-1	803-000067-313	Transceiver, optical, SFP, longwave laser, LC connector, 35 km, 2.125 Gbps	0 to 12

Miscellaneous Parts

Figure 6-2 illustrates miscellaneous parts. Table 6-2 is the associated parts list. The table includes reference numbers to Figure 6-2, part numbers, descriptions, and quantities.

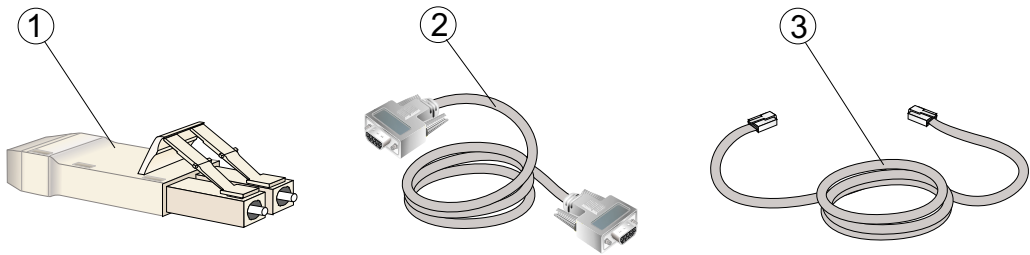


Figure 6-2 Miscellaneous Parts

Table 6-2 Miscellaneous Parts List

Ref.	Part Number	Description	Qty.
-1	803-000057-000	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
-1	803-000057-001	Plug, loopback, LC connector, singlemode, 9/125 micron (#1149)	1
-2	801-000039-000	Cable, null modem, DB9F-DB9F connector	1
-3	801-000035-010	Cable, Ethernet, 10-foot	1

Power Cords and Receptacles

Figure 6-3 illustrates optional power cords and receptacles. Table 6-3 on page 6-5 is the associated parts list. The table includes reference numbers to Figure 6-3, feature numbers, and descriptions.


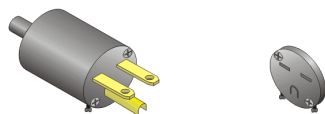
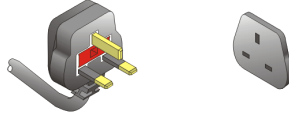
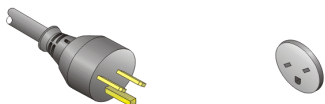
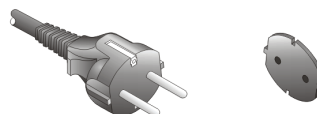


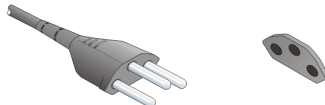
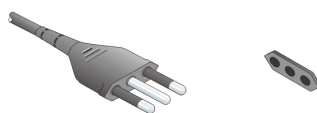
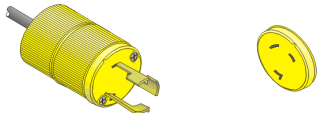


1		7, 11,15	
2		8	
3		9	
4		10	
5		12, 13,14	
6		16	

Figure 6-3 Power Cords and Receptacles

Table 6-3 Power Cord and Receptacle List

Ref.	Part Number	Description	Feature
-1	806-000001-000	Power cord, AC, North America NEMA 5-15P straight, 125 volts, 10 amps, 3.0 meters Receptacle: NEMA 5-15R	1010
-2	806-000004-001	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
-3	806-000005-001	Power cord, AC, European Community CEE 7/7 straight, 250 volts, 10 amps, 2.5 meters Receptacle: CEE 7	1013
-4	806-000006-001	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
-5	806-000027-000	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
-6	806-000029-000	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
-7	806-000030-000	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
-8	806-000033-000	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
-9	806-000034-000	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
-10	806-000037-000	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
-11	806-000038-000	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027

Table 6-3 Power Cord and Receptacle List (Continued)

Ref.	Part Number	Description	Feature
-12	806-000040-000	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028
-13	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016
-14	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1029
-15	806-000043-000	Power cord, AC, Japan NEMA 6-15P straight, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA 6-15R	None
-16	806-000058-000	Power cord, AC, Japan JIS 8303 straight, 125 volts, 12 amps, 2.5 meters Receptacle: NEMA 5-15R	1030

Event Code Tables

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Events are reported as event codes.

This appendix lists all three-digit event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format, and are grouped as follows:

- 000 through 199 - system events.
- 300 through 399 - fan events.
- 400 through 499 - control processor (CTP) card events.
- 500 through 599 - port events.
- 800 through 899 - thermal sensor events.

Events are recorded in the event log of the SANpilot interface or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error (**ERR**) light-emitting diode (LED) at the switch front panel.

In addition to numerical event codes, the tables in this appendix also provide a:

- **Message** - a brief text string that describes the event.
- **Severity** - a severity level that indicates event criticality as follows:
 - 0 - informational.
 - 2 - minor.
 - 3 - major.
 - 4 - severe (not operational).
- **Explanation** - a complete explanation of what caused the event.
- **Action** - the recommended course of action (if any) to resolve the problem.
- **Event data** - supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution** - check marks in associated fields indicate where the event code is reported (switch or attached host).

System Events (000 through 199)

Event Code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All fabric services databases initialize to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓					

Event Code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed its CRC validation. All fabric services databases initialize to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓					

Event Code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the SANpilot interface are allowed.						
Action:	Add the community name to the SNMP configuration using the SANpilot interface.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 051

Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed its CRC validation. All management services databases initialize to an empty state, resulting in an implicit logout of all devices logged in to the Management Server.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓					

Event Code: 052							
Message:	Management Server internal error, asynchronous status report activation, or mode register update occurred.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the Management Server subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.						
Action:	<p>Management Server internal error: Perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>Asynchronous status report activation: No action required.</p> <p>Mode register update: No action required.</p>						
Event Data:	<p>Supplementary data consists of reporting tasks of type eMST_SB2, with component_id eMSCID_SB2_CHPGM. For each type of error or indication, the subcomponent_id is:</p> <p>Management Server internal error: subcomponent_id is eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR or eMS_ELR_SB2_MSG_PROCESSING_ERROR.</p> <p>Asynchronous status report activation: subcomponent_id is eSB2_CP_RER_ASYNC_STATUS_REPORTING.</p> <p>Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓					✓	

Event Code: 061

Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the fabric controller database failed its CRC validation. All fabric controller databases initialize to an empty state, resulting in a momentary loss of interswitch communication.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓					

Event Code: 062

Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (director or switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two directors or switches traverses no more than seven ISLs.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) more than seven hops away.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this switch.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) with too many ISLs.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 070

Message: E_Port is segmented.

Severity: Informational.

Explanation: A switch E_Port recognized an incompatibility with the attached fabric director or switch, preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic, but transmits Class F traffic. Refer to the event data for the segmentation reason.

Action: Action depends on the segmentation reason specified in the event data.

Event Data: The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows:

1 = Incompatible operating parameters - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric elements.

2 = Duplicate domain ID - The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.

3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.

4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.

5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.

6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the diskette to McDATA support personnel.

Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 071							
Message:	Switch is isolated.						
Severity:	Informational.						
Explanation:	The switch is isolated from other fabric elements (directors or switches). This event code is accompanied by one or more 070 event codes. Refer to the event data for the segmentation reason.						
Action:	Action depends on the segmentation reason specified in the event data.						
Event Data:	<p>The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:</p> <p>1 = Incompatible operating parameters - Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric elements.</p> <p>2 = Duplicate domain ID - The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.</p> <p>3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p>4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p>6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the diskette to McDATA support personnel.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 072

Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 073

Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	Byte 0 = error reason code for engineering evaluation. Bytes 4 - 9 = port numbers for which problems were detected.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (073 event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Bytes 4 - 8 = Count of frame delivery timeouts. Bytes 9 - 11 = Count of frame delivery aborts.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The WWN of the device or fabric element connected to the indicated port is not authorized for that port number.						
Action:	Change the port binding definition or connect the proper device or fabric element to the indicated port.						
Event Data:	Byte 0 = Port number reporting the unauthorized connection. Bytes 4 - 11 = WWN of the unauthorized device or fabric element.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓					✓	

Event Code: 081

Message: Invalid attachment.

Severity: Informational.

Explanation: A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.

Action: Action depends on the reason specified in the event data.

Event Data: The first byte of event data (byte 0) specifies the port number. The fifth byte (byte 4) specifies the isolation reason as follows:

1 = Unknown - Isolation reason is unknown, but probably caused by failure of a device attached to the switch through an **E_Port** connection. Fault isolate the failed device or contact support personnel to report the problem.

2 = ISL connection not allowed - The port connection conflicts with the configured port type. Change the port type to **F_Port** if the port is cabled to a device, or **E_Port** if the port is cabled to a fabric element to form an ISL.

3 = Incompatible switch - The switch returned a *Process ELP Reject - Unable to Process* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

4 = Incompatible switch - The switch returned a *Process ELP Reject - Invalid Revision Level* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

5 = Loopback plug connected - A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug.

6 = N_Port connection not allowed - The switch is connected to a fabric element through a port configured as an **F_port**. Change the port type to **E_Port**.

7 = Non-McDATA switch at other end - The attached fabric element is not a McDATA product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor.

A = Unauthorized port binding WWN - The device WWN or nickname used to configure port binding for this port is not valid. At the *Configure Ports* dialog box, reconfigure the port with the WWN or nickname authorized for the attached device.

B = Unresponsive node - The attached node did not respond, resulting in a **G_Port** ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

Event Code: 081 (continued)							
Event Data (continued):	<p>C = ESA security mismatch - Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and switch binding parameters for this switch and the attached fabric element must agree. At the <i>Fabric Binding</i> and <i>Switch Binding - State Change</i> dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.</p> <p>D = Fabric binding mismatch - Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the <i>Fabric Binding</i> dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.</p> <p>E = Authorization failure reject - The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.</p> <p>F = Unauthorized switch binding WWN - Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the <i>Switch Binding - Membership List</i> dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.</p> <p>11 = Fabric mode mismatch - Based on the ELP revision level, a connection was not allowed because a McDATA switch in legacy mode is attached to a McDATA switch in Open Fabric mode, or a McDATA switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the <i>Interop Mode</i> drop-down list at the <i>Configure Fabric Parameters</i> dialog box.</p> <p>12 = CNT WAN extension mode mismatch - Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. Contact McDATA support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow McDATA switches to communicate with CNT UltraEdge WAN Gateways.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives an management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this switch and return the diskette to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 142

Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 143

Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 150	
Message:	Zone merge failure.
Severity:	Informational.
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a 070 ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.
Action:	Action depends on the failure reason specified in the event data.
Event Data:	<p>Bytes 0 - 3 of the event data specify affected E_Port number(s). Bytes 8 - 11 specify the failure reason as follows:</p> <p>01 = Invalid data length - An invalid data length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>08 = Invalid zone set format - An invalid zone set format caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>09 = Invalid data - Invalid data caused a zone merge failure. Inspect bytes 12 - 15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem.</p> <p>0A = Cannot merge - A <i>Cannot Merge</i> condition caused a zone merge failure. Inspect bytes 12 - 15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem.</p> <p>F0 = Retry limit reached - A retry limit reached condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>F1 = Invalid response length - An invalid response length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p> <p>F2 = Invalid response code - An invalid response code caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the diskette to McDATA support personnel.</p>

Event Code: 150 (continued)

Event Data
(continued):

Bytes **12 - 15** of the event data specify error codes as follows:

01 = Completion fail.

03 = Zone merge error - too many zones.

04 = Zone merge error - incompatible zones.

05 = Zone merge error - too long if reason = **0A**.

06 = Zone set definition too long.

07 = Zone set name too short or not authorized.

08 = Invalid number of zones.

09 = Zone merge error - default zone states incompatible if reason = **0A**.

0A = Invalid protocol.

0B = Invalid number of zone members.

0C = Invalid flags.

0D = Invalid zone member information length.

0E = Invalid zone member information format.

0F = Invalid zone member information port.

10 = Invalid zone set name length.

11 = Invalid zone name length.

37 = Invalid zone name.

39 = Duplicate zone.

3C = Invalid number of zone members.

3D = Invalid zone member type.

3E = Invalid zone set name.

45 = Duplicate member in zone.

4A = Invalid number of zones.

4B = Invalid zone set size.

4D = Maximum number of unique zone members exceeded.

Distribution:

Switch

Management Server

Host

SANpilot
Event Log

System
Error LED

Event Log

E-Mail

Call-Home

Sense Info

Link Incident

✓

✓

Event Code: 151							
Message:	Fabric configuration failure.						
Severity:	Informational.						
Explanation:	A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	<p>Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:</p> <p>Bytes 0 - 3 = Managing switch domain ID in internal format (1-31). Bytes 4 - 7 = Fabric configuration operation that failed. Bytes 8 - 11 = Fabric configuration step that failed. Bytes 12 - 15 = Managed switch domain ID in internal format (1-31). Bytes 16 - 19 = Response command code received from the managed switch. Bytes 20 - 23 = Response code received from the managed switch. Bytes 24 - 27 = Reason code received from the managed switch. Bytes 28 - 31 = Error code received from the managed switch.</p>						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓					

Fan Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of three) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly associated with the failed fan.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 302							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of three) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the power supply assembly (or assemblies) associated with the failed fans.						
Action:	Replace the switch.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of three) recovered or the associated power supply assembly was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 311

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of three) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 312

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of three) recovered or the associated power supply assembly (or assemblies) were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers (0 through 2 inclusive).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a failed FRU as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, replace the power supply assembly. Perform the data collection procedure and return the diskette and faulty FRU to McDATA support personnel.						
Event Data:	Byte 0 = FRU code as follows: 02 = CTP card, 05 = cooling fan, 06 = power supply assembly. Byte 1 = FRU slot number.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code 411), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte 0 = reset type as follows: 00 = power-on, 02 = IML, 04 = reset.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	<p>Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers from the switch to the server, where it is stored for later retrieval through the data collection procedure.</p> <p>The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.</p>						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	Bytes 0 - 3 = fault identifier, least significant byte first.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 412							
Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel.						
Event Data:	Byte 0 = reset type as follows: 00 = task switch did not occur within approximately one second, 01 = interrupt servicing blocked for more than approximately one second.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A new firmware version was downloaded to the switch from the SANpilot interface. Event data contains the ASCII firmware version in hexadecimal format xx.yy.zz.bbbb .						
Action:	No action required.						
Event Data:	Bytes 0 and 1 = release level (xx). Bytes 6 and 7 = interim release level (zz). Byte 2 = always a period. Byte 8 = always a space. Bytes 3 and 4 = maintenance level (yy). Bytes 9 - 12 = build ID (bbbb). Byte 5 = always a period.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The SANpilot interface initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 426

Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a 426 event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte 0 of the event data (equal to 5 , 10 , 15 , or 20) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to 10 indicates 1,024 ECC error interrupts.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 433

Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte 0 = LAN error type as follows: 01 = hard failure, 04 = registered fault. Byte 1 = LAN error subtype (internally defined). Byte 2 = LAN fault identifier (internally defined).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal error.						
Action:	Replace the switch.						
Event Data:	Byte 0 = CTP slot position (00). Byte 1 = engineering reason code Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 445							
Message:	ASIC detected a system anomaly.						
Severity:	Informational.						
Explanation:	The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.						
Event Data:	Byte 0 = embedded port number. Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the SANpilot interface. The switch performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	Byte 0 = feature description as follows: 00 - 04 = Flexport Technology, 06 = Open-system management server. Byte 1 = feature description as follows: 06 = SANtegrity binding, 07 = OpenTrunking.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Port Events (500 through 599)

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific. Byte 16 = connector type. Bytes 17 and 18 = transmitter technology. Byte 19 = distance capabilities. Byte 20 = supported transmission media. Byte 21 and 22 = speed capability and configuration.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code 506 is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific. Byte 12 = test type.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 508							
Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code 506 is generated if this anomaly results in a hard port failure.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = anomaly reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 510							
Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an SFP optical transceiver was initiated with the switch powered on and operational. The event indicates operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 11) Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 512							
Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 513							
Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 11) Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 514

Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 523

Message:	FL_Port open request failed.						
Severity:	Informational.						
Explanation:	When the indicated FL_Port attempted to open a loop device, the port open (OPN) sequence was returned.						
Action:	No action required.						
Event Data:	Byte 0 = port number (00 - 11). Byte 1 = arbitrated loop physical address (AL_PA) of the device transmitting the OPN sequence.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 524							
Message:	No AL_PA acquired.						
Severity:	Informational.						
Explanation:	Switch cannot allocate an AL_PA of 0 (loop master) for an FC-AL device during loop initialization. The device cannot participate in loop operation.						
Action:	Disconnect the FC-AL device that is loop master.						
Event Data:	Byte 0 = port number (00 - 11).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 525							
Message:	FL_Port arbitration timeout.						
Severity:	Informational.						
Explanation:	A switch port could not win loop arbitration within the specified loop protocol time out value (LP_TOV).						
Action:	Switch firmware reinitializes the arbitrated loop. No user action required.						
Event Data:	Byte 0 = port number (00 - 11).						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓						

Event Code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached open systems interconnection (OSI) server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 582							
Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 585

Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 586

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to MAP 0000: Start MAP on page 3-6 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Thermal Sensor Events (800 through 899)

Event Code: 810							
Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP2 card indicates the warm temperature threshold was reached or exceeded.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 811							
Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP2 card indicates the hot temperature threshold was reached or exceeded.						
Action:	Perform the data collection procedure and return the diskette to McDATA support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

A

- AC power receptacle, location [1-3](#)
- applications
 - diagnostic features [1-11](#)
 - SANpilot interface [1-11](#)
- attention statements [xvii](#)

B

- binding
 - fabric
 - configure [2-32](#)
 - description [2-32](#)
 - port
 - configure [2-26](#)
 - description [2-26](#)
 - switch
 - configure [2-27](#)
 - description [2-27](#)
- block ports [4-26](#)

C

- clean fiber-optic components [4-28](#)
- clear
 - event log entries [4-6, 4-7, 4-8, 4-10, 4-11](#)
- clearances [1-7](#)
- command line interface
 - disable [2-23](#)
 - enable [2-23](#)
- compliance statements
 - Class 1 laser transceiver [xvi](#)
 - CNS mark [xvi](#)

- European Union conformity declarations
 - [xvii](#)
- European Union directives [xvii](#)
- Federal Communications Commission [xvi](#)
- configure
 - fabric binding [2-32](#)
 - fabric parameters [2-16](#)
 - OpenTrunking [2-35](#)
 - passwords [2-25](#)
 - PFE key [2-38](#)
 - port binding [2-26](#)
 - ports [2-8](#)
 - SNMP [2-21](#)
 - switch binding [2-27](#)
 - switch date and time [2-13](#)
 - switch identification [2-11](#)
 - switch network information [2-19, 2-39](#)
 - switch operating parameters [2-14](#)
 - user names [2-25](#)
 - zone sets [2-46](#)
 - zones [2-46](#)
- cooling fan
 - description [1-4](#)
 - events (300 - 399) [A-20](#)
 - fault isolation [3-30](#)
- CTP card
 - events (400 - 499) [A-23](#)
 - fault isolation [3-30](#)
 - firmware versions [4-32](#)

D

- danger statements [xvii](#)
- date, set at switch [2-13](#)

- default
 - maintenance port password [2-43](#)
 - SANpilot interface password [2-8](#)
 - SANpilot interface user name [2-8](#)
 - switch gateway address [2-1](#), [3-1](#)
 - switch IP address [2-1](#), [3-1](#)
 - switch passwords [2-1](#), [3-1](#)
 - switch subnet mask [2-1](#), [3-1](#)
- dimensions [1-7](#)
- disable
 - EFM [2-34](#)
 - OSMS [2-24](#)
- download firmware [4-38](#)
- E**
- E_D_TOV [2-17](#)
- E_Port
 - configuring [2-8](#)
 - description [1-2](#)
 - PFE key requirement [1-2](#)
 - segmented [3-54](#)
- enable
 - EFM [2-34](#)
 - OSMS [2-24](#)
- enterprise fabric mode
 - disable [2-34](#)
 - enable [2-34](#)
- environment
 - operating [1-8](#)
 - shipping [1-8](#)
 - storage [1-8](#)
- ERR LED
 - description [1-6](#)
 - location [1-3](#)
- error
 - log, clearing [4-6](#), [4-7](#), [4-8](#), [4-10](#), [4-11](#)
- error detection
 - description [1-10](#)
 - event codes [3-3](#)
 - SANpilot interface [1-11](#)
- error reporting
 - description [1-10](#)
 - event codes [3-3](#)
 - SANpilot interface [1-11](#)
- ESD precautions [xx](#)
- Ethernet connector
 - description [1-6](#)
 - location [1-3](#)
- event codes
 - cooling fan events (300 - 399) [A-20](#)
 - CTP card events (400 - 499) [A-23](#)
 - description [A-2](#)
 - port events (500 - 599) [A-29](#)
 - system events (000 - 199) [A-2](#)
 - thermal sensor events (800 - 899) [A-37](#)
- Event Log
 - description [4-4](#)
 - illustration [4-3](#)
- event log [4-6](#), [4-7](#), [4-8](#), [4-9](#), [4-10](#)
 - clearing [4-6](#), [4-7](#), [4-8](#), [4-10](#), [4-11](#)
- external loopback test
 - description [4-19](#)
 - procedure [4-21](#)
- F**
- F_Port
 - configuring [2-8](#)
 - description [1-2](#)
- fabric binding
 - configure [2-32](#)
 - description [2-32](#)
- fabric parameters, configure [2-16](#)
- Fabriccenter equipment cabinet
 - description [1-2](#)
 - switch installation [2-5](#)
- fault isolation
 - MAP 0000 - Start MAP [3-6](#)
 - MAP 0100 - Power distribution analysis [3-18](#)
 - MAP 0200 - POST failure analysis [3-21](#)
 - MAP 0300 - Loss of web browser PC communication [3-23](#)
 - MAP 0400 - FRU failure analysis [3-30](#)
 - MAP 0500 - Port failure and link incident analysis [3-35](#)
 - MAP 0600 - Fabric, ISL, and segmented port problem determination [3-54](#)
 - summary [3-2](#)
- FCC compliance statement [xvi](#)
- fiber-optic protective plug
 - description [1-14](#)
 - illustration [1-14](#)
- firmware

- add version to browser PC [4-33](#)
 - determine version [4-32](#)
 - download [4-38](#)
 - FL_Port
 - configuring [2-8](#)
 - description [1-2](#)
 - FRU removal
 - SFP transceiver [5-2](#)
 - tools required [5-2](#)
 - FRU replacement
 - SFP transceiver [5-4](#)
 - tools required [5-2](#)
 - FRUs
 - description [1-3](#)
 - illustrated parts breakdown [6-1](#)
 - SFP transceiver [1-4](#)
 - status LEDs [1-6](#)
 - full-volatility feature [4-23](#)
- G**
- gateway address
 - change switch address [2-19](#), [2-40](#)
 - switch default [2-1](#), [3-1](#)
- H**
- heat dissipation [1-7](#)
- I**
- illustrated parts breakdown
 - front-accessible FRUs [6-2](#)
 - miscellaneous parts [6-3](#)
 - power cord [6-4](#)
 - IML switch [4-31](#)
 - IML/Reset button
 - function [1-5](#)
 - location [1-3](#)
 - insistent domain ID [2-15](#)
 - installation options
 - customer-supplied rack [2-2](#)
 - desktop [2-2](#)
 - Fabricenter cabinet [2-2](#)
 - installation tasks
 - summary [2-2](#)
 - Task 1 - Verify installation requirements [2-3](#)
 - Task 2 - Unpack, inspect, and install the switch [2-3](#)
 - Task 3 - Configure the switch at the SANpilot interface [2-6](#)
 - Task 4 - Configure switch network information [2-39](#)
 - Task 5 - Cable Fibre Channel ports [2-45](#)
 - Task 6 - Configure zoning (optional) [2-46](#)
 - Task 7 - Connect switch to a fabric element (optional) [2-51](#)
 - Task 8 - Register with the McDATA file center [2-52](#)
 - internal loopback test
 - description [4-19](#)
 - procedure [4-19](#)
 - interop mode [2-18](#)
 - interswitch link
 - description [1-2](#)
 - fault isolation [3-54](#)
 - IP address
 - change switch address [2-19](#), [2-39](#)
 - switch default [2-1](#), [3-1](#)
- L**
- laser transceiver
 - compliance statement [xvi](#)
 - description [1-4](#)
 - illustrated parts breakdown [6-2](#)
 - removal [5-2](#)
 - replacement [5-4](#)
 - types available [1-4](#)
 - LEDs
 - ERR [1-6](#)
 - port status [1-6](#), [4-11](#)
 - PWR [1-6](#)
 - Link Incident Log
 - description [4-5](#)
 - illustration [4-5](#)
 - list
 - switch binding membership [2-28](#)
 - log
 - clearing [4-6](#), [4-7](#), [4-8](#), [4-10](#), [4-11](#)
 - events [4-6](#), [4-7](#), [4-8](#), [4-9](#), [4-10](#)
 - Log tab view [4-6](#), [4-7](#), [4-8](#), [4-9](#), [4-10](#)
 - logs
 - clear [4-2](#)

- Event Log [4-3](#)
- Link Incident Log [4-5](#)
- Open Trunking Re-Route Log [4-4](#)
- loopback plug
 - description [1-14](#)
 - illustration [1-14](#)
- loopback test
 - description [4-19](#)
 - external [4-21](#)
 - internal [4-19](#)

M

- MAC address, switch [2-39](#)
- maintenance analysis procedures
 - MAP 0000 - Start MAP [3-6](#)
 - MAP 0100 - Power distribution analysis [3-18](#)
 - MAP 0200 - POST failure analysis [3-21](#)
 - MAP 0300 - Loss of web browser PC
 - communication [3-23](#)
 - MAP 0400 - FRU failure analysis [3-30](#)
 - MAP 0500 - Port failure and link incident
 - analysis [3-35](#)
 - MAP 0600 - Fabric, ISL, and segmented port
 - problem determination [3-54](#)
 - summary [3-2](#)
- maintenance approach [1-8](#)
- maintenance port
 - configure switch network addresses [2-40](#)
 - default password [2-43](#)
 - description [1-6](#)
 - location [1-3](#)
- management, through SANpilot interface [1-10](#)
- membership list
 - switch binding [2-28](#)
- monitoring
 - events [4-6, 4-7, 4-8, 4-9, 4-10](#)

N

- network information
 - configure switch [2-39](#)
 - configure switch at SANpilot interface [2-19](#)
- null modem cable
 - description [1-14](#)
 - illustration [1-15](#)

O

- offline state, set [4-26](#)
- online state, set [4-25](#)
- Open Trunking Re-Route Log
 - description [4-4](#)
 - illustration [4-4](#)
- open-systems management server
 - disable [2-24](#)
 - enable [2-24](#)
- OpenTrunking
 - configure [2-35](#)
- operating environment [1-8](#)
- operating parameters, configure [2-14](#)

P

- password
 - configure for SANpilot interface [2-25](#)
 - customer-level switch [2-1, 3-1](#)
 - default maintenance port [2-43](#)
 - default SANpilot interface [2-8](#)
 - maintenance-level switch [2-1, 3-1](#)
- performance statistics
 - Class 2 [4-17](#)
 - Class 3 [4-17](#)
 - errors [4-16](#)
 - traffic [4-16](#)
- PFE keys
 - configure [2-38](#)
- port binding
 - configure [2-26](#)
 - description [2-26](#)
- ports
 - block [4-26](#)
 - cabling [2-45](#)
 - configurable types [1-1](#)
 - configure [2-8](#)
 - diagnostics [4-11](#)
 - events (500 - 599) [A-29](#)
 - loopback test [4-19](#)
 - performance statistics [4-15](#)
 - port properties [4-17](#)
 - port technology [4-17](#)
 - SFP transceivers [1-4](#)
 - status LEDs [4-11](#)
 - unblock [4-26](#)
- power cord

- connecting 2-5
- illustrated parts breakdown 6-4
- power requirements 1-7
- power supply
 - description 1-4
 - fault isolation 3-18
- power-off procedure 4-30
- power-on procedure 4-29
- precautions
 - ESD xx
 - general xx
- preferred domain ID 2-14
- procedural notes 4-2, 5-1
- procedures
 - data collection 4-22
 - fault isolation 3-1
 - FRU remove and replace 5-2
 - installation 2-2
 - power-off 4-30
 - power-on 4-29
 - repair 4-1
- publications, related xiv
- PWR LED
 - description 1-6
 - location 1-3

R

- R_A_TOV 2-17
- related publications xiv
- remove and replace procedures 5-2
- repair procedures
 - block or unblock a port 4-26
 - clean fiber-optic components 4-28
 - collect maintenance data 4-22
 - IML or reset the switch 4-30
 - manage firmware versions 4-32
 - obtain log information 4-2
 - obtain port diagnostic information 4-11
 - perform port diagnostic loopback tests 4-19
 - power-off procedure 4-30
 - power-on procedure 4-29
 - reset configuration data 4-40
 - set the switch online or offline 4-25
- rerouting delay 2-15
- reset
 - configuration data 4-40

- switch 4-31

S

- safety
 - attention statements xvii
 - danger statements xvii
 - ESD precautions xx
 - general precautions xx
- SANpilot interface
 - configure switch 2-6
 - default display 1-11
 - description 1-10
 - event code tables A-1
 - Event Log 4-3
 - Link Incident Log 4-5
 - Open Trunking Re-Route Log 4-4
- segmented E_Port
 - description 2-15
 - fault isolation 3-54
- serviceability features 1-10
- SFP transceiver
 - description 1-4
 - fault isolation 3-35
 - illustrated parts breakdown 6-2
 - removal 5-2
 - replacement 5-4
 - types available 1-4
- shipping environment 1-8
- SNMP
 - configure 2-21
 - description 1-13
 - traps 1-13
- software
 - diagnostic features 1-11
 - SANpilot interface 1-11
- Solution Center
 - e-mail address xiv
 - fax number xiv
 - phone number xiv
- specifications
 - heat dissipation 1-7
 - switch clearances 1-7
 - switch dimensions 1-7
 - switch power requirements 1-7
- Sphereon 4300 Switch
 - description 1-1

- firmware [4-32](#)
- FRU removal and replacement [5-1](#)
- FRUs [1-3](#)
- illustrated parts breakdown [6-1](#)
- illustration [1-2](#)
- installation [2-3](#)
- installation options [2-2](#)
- maintenance analysis procedures [3-1](#)
- maintenance approach [1-8](#)
- management [1-9](#)
- repair procedures [4-1](#)
- specifications [1-7](#)
- storage environment [1-8](#)
- subnet mask
 - change switch value [2-19](#), [2-40](#)
 - switch default [2-1](#), [3-1](#)
- switch binding
 - configure [2-27](#)
 - description [2-27](#)
- switch binding membership list
 - configuring [2-31](#)
 - overview [2-28](#)
- switch identification, configure [2-11](#)
- switch priority [2-17](#)
- system events (000 - 199) [A-2](#)

T

- technical support
 - Solution Center e-mail address [xiv](#)
 - Solution Center fax number [xiv](#)
 - Solution Center phone number [xiv](#)
- thermal sensor events (800 - 899) [A-37](#)
- time, set at switch [2-13](#)
- tools and test equipment
 - FRU removal and replacement [5-2](#)
 - supplied by service personnel [1-15](#)
 - supplied with switch [1-14](#)
- trademarks [xv](#)

U

- unblock ports [4-28](#)
- user name
 - configure for SANpilot interface [2-25](#)
 - default SANpilot interface [2-8](#)

Z

- zone sets
 - configure [2-49](#)
 - description [2-46](#)
- zones
 - add or delete members [2-48](#)
 - configure [2-46](#)
 - description [2-46](#)